UNIVERSITY OF KWAZULU-NATAL

SCHOOL OF LAW – HOWARD COLLEGE

Privacy by (re)Design: A Comparative Study of the Protection of Personal Information in the Mobile Applications Ecosystem under United States, European Union and South African Law

Dusty-Lee Donnelly

(Student number: 951028800)

This thesis is submitted in pursuance of the requirements for the degree of Doctor of Laws

Supervisor: Dr DW Thaldar

Co-Supervisor: Mr AH Bellengère

2020

DECLARATION REGARDING ORIGINALITY

I, **Dusty-Lee Donnelly**, with student number **951028800**, hereby declare that:

A. The research reported in this dissertation, except where otherwise indicated, is my original research.

B. This dissertation has not been submitted for any degree or examination at any other university.

C. This dissertation does not contain other persons' data, pictures, graphs or other information, unless specifically acknowledged as being sourced from other persons.

D. This dissertation does not contain other persons' writing, unless specifically acknowledged as being sourced from other researchers. Where other written sources have been quoted, then:

    a. their words have been re-written, but the general information attributed to them has been referenced;

    b. where their exact words have been used, their writing has been placed inside quotation marks, and referenced.

E. Where I have reproduced a publication of which I am an author, co-author or editor, I have indicated in detail which part of the publication was written by myself alone and have fully referenced such publications.

F. This dissertation does not contain text, graphics or tables copied and pasted from the Internet, unless specifically acknowledged, and the sources being detailed in the dissertation/thesis and in the References sections.

Signed: _____

Date: _____

ABSTRACT

The dissertation presents a comparative desktop study of the application of a Privacy by Design (PbD) approach to the protection of personal information in the mobile applications ecosystem under the Children's Online Privacy Protection Act (COPPA) and the California Consumer Protection Act (CCPA) in the United States, the General Data Protection Regulation (GDPR) in the European Union, and the Protection of Personal Information Act (POPIA) in South Africa.

The main problem considered in the thesis is whether there is an 'accountability gap' within the legislation selected for comparative study. This is analysed by examining whether the legislation can be enforced against parties other than the app developer in the mobile app ecosystem, as it is theorised that only on this basis will the underlying technologies and architecture of mobile apps be changed to support a privacy by (re)design approach. The key research question is what legal approach is to be adopted to enforce such an approach within the mobile apps ecosystem.

It describes the complexity of the mobile apps ecosystem, identifying the key role players and the processing operations that take place.

It sets out what is encompassed by the conceptual framework of PbD, and why the concept of privacy by (re)design may be more appropriate in the context of mobile apps integrating third party services and products. It identifies the core data protection principles of data minimisation and accountability, and the nature of informed consent, as being essential to an effective PbD approach.

It concludes that without strengthening the legal obligations pertaining to the sharing of personal information with third parties, neither regulatory guidance, as is preferred in the United States, nor a direct legal obligation, as created by article 25 of the GDPR, is adequate to enforce a PbD approach within the mobile apps ecosystem. It concludes that although a PbD approach is implied for compliance by a responsible party with POPIA, legislative reforms are necessary. It proposes amendments to POPIA to address inadequacies in the requirements for notice, and to impose obligations on a responsible party in relation to the sharing of personal information with third parties who will process the personal information for further, separate purposes.

DEDICATION AND ACKNOWLEDGEMENTS

This dissertation is dedicated to my late father, Geoffrey Michael Weatherhead, who taught me to embrace the value of a curious mind.

It would not have been possible without the unwavering love and support of my husband, Martin. I am also very grateful for the critical guidance of Dr Donrich Thaldar, Prof Tana Pistorius and Mr Adrian Bellengère, and two colleagues who also provided a sounding board for my ideas and much needed moral support, Dr Lee Swales and Mr Eben van der Merwe.

To the app developers and entrepreneurs who took part in the preliminary studies conducted into mobile app development in South Africa, thank you for generously sharing your experiences with me. The financial assistance of the National Research Foundation (NRF) University Capacity Development Programme (UCDP) is hereby gratefully acknowledged. Opinions expressed and conclusions arrived at are those of the author and are not to be attributed to the NRF.

TABLE OF CONTENTS

DECLARATION REGARDING ORIGINALITY i
ABSTRACT ii
DEDICATION AND ACKNOWLEDGEMENTS iii
LIST OF ABBREVIATIONS xi
TABLE OF TABLES xii
TABLE OF FIGURES xii
CHAPTER 1 1
INTRODUCTION *1*
I THE FUTURE IS DATA-DRIVEN *1*
II THE ADVENT OF MOBILE APPLICATIONS *4*
III NEW RISKS TO PRIVACY *6*
IV NATURE AND EXTENT OF THE RISK *9*
V LEGISLATIVE COMPLEXITY AND THE GOAL OF HARMONISATION *14*
VI PRIVACY BY DESIGN AS A HARMONISING PRINCIPLE: A LITERATURE REVIEW *16*
VII REGULATORY APPROACHES TO PRIVACY BY DESIGN IN RELATION TO MOBILE APPS *21*
VIII STUDY RATIONALE *26*
IX STUDY HYPOTHESIS AND KEY RESEARCH QUESTIONS *29*
X METHODOLOGY *31*
XI CHAPTER BREAKDOWN *33*
XII KEY TERMINOLOGY *34*
XIII CONCLUSION *37*
CHAPTER 2 41
THE MOBILE APPLICATIONS ECOSYSTEM *41*
I INTRODUCTION *41*
II DEFINITION OF KEY CONCEPTS *43*
(A) THE MOBILE APPLICATION *43*
(B) THE USER INTERFACE (UI) AND USER EXPERIENCE (UX) *44*
(C) THE APPLICATION PROCESSING INTERFACE (API) *44*
(D) THIRD PARTY LIBRARY *45*
(E) SOFTWARE DEVELOPMENT KIT (SDK) *46*
(F) THE OPERATING SYSTEM *46*
(G) PERMISSIONS *46*
(H) BROADCASTS *48*
(I) BACKGROUND PROCESSING *48*
(J) THE DEVICE (HARDWARE) *49*

(K) THE MOBILE APPLICATIONS ECOSYSTEM 50
III PRINCIPAL PARTIES IN THE MOBILE APPLICATIONS ECOSYSTEM 51
(A) THE USER 51
(B) THE APP DEVELOPER 52
IV GATEKEEPERS IN THE APP ECOSYSTEM 54
(A) THE APP MARKETPLACE 54
(B) THE OWNER OF THE OPERATING SYSTEM 56
(C) ELECTRONIC COMMUNICATIONS SERVICE PROVIDER (ECSP) 57
(D) MOBILE NETWORK OPERATOR (MNO) 57
(E) INTERNET SERVICE PROVIDER (ISP) 57
(F) DEVICE MANUFACTURERS 58
(G) ONLINE SOCIAL NETWORK (OSN) PLATFORMS 60
V THIRD PARTIES IN THE MOBILE APPLICATIONS ECOSYSTEM 63
(A) BACK-END SERVICE PROVIDERS 64
(B) ANALYTICS COMPANIES 65
(C) DATA BROKERS 66
(D) ADVERTISING NETWORKS 67
(E) ADVERTISING EXCHANGES 70
VI DATA PROCESSING IN THE MOBILE APPLICATIONS ECOSYSTEM 71
(A) DATA 71
(B) METADATA 71
(C) LOCATION DATA 73
(D) DEVICE FINGERPRINTING (WHAT HAPPENED TO THE COOKIES?) 75
(E) DATA LIFECYCLE 76
(F) BIG DATA 76
(G) DATA SHARING 77
(H) RAW DATA 78
(I) AGGREGATED DATA 78
(J) DE-IDENTIFIED (ANONYMOUS) DATA 78
(K) PSEUDONYMISED DATA (WHY HAS MY DATA BEEN HASHED?) 79
(L) ENCRYPTED DATA 80
(M) DATA MINING 83
(N) DATA LEAKS AND DATA BREACHES 83
(O) PERSONALISATION 84
(P) PROFILING AND INFORMATION MATCHING 85
(Q) NUDGING 86
VII PERSONAL INFORMATION COLLECTED BY MOBILE APPS 86

VIII ONLINE ADVERTISING: GENERIC, CONTEXTUAL AND TARGETED ADVERTISEMENTS 88
IX THE MOBILE "CLOUD" 94
X CONCLUSION 96
CHAPTER 3 98
'PRIVACY BY (RE)DESIGN' IN ITS INTERNATIONAL, REGIONAL AND NATIONAL CONTEXT 98
I INTRODUCTION 98
II CORE DATA PROTECTION PRINCIPLES 100
III DATA PROTECTION IN ITS INTERNATIONAL, REGIONAL AND NATIONAL CONTEXT 103
IV THE CONCEPTUAL FRAMEWORK OF PRIVACY BY DESIGN (PBD) 105
V THE NATURE OF PRIVACY BY DESIGN 111
IX PRIVACY BY (RE)DESIGN 113
VI PRIVACY BY DESIGN AND THE ACCOUNTABILITY PRINCIPLE 114
VII PRIVACY BY DESIGN AND THE PRINCIPLE OF MINIMALITY 116
VIII PRIVACY BY DESIGN AND THE CONCEPT OF INFORMED CONSENT 118
X CONCLUSION 120
CHAPTER 4 121
US DATA PROTECTION LAW 121
I INTRODUCTION 121
II THE FEDERAL POSITION: A SECTORAL APPROACH 123
III FAIR INFORMATION PRACTICE PRINCIPLES (FIPPS) 127
IV THE CHILDREN'S ONLINE PRIVACY PROTECTION ACT (1998) (COPPA) 130
(A) ORIGIN AND BACKGROUND 130
(B) PERSONAL INFORMATION 131
(C) OPERATOR 133
(D) DATA PROTECTION PRINCIPLES 136
(E) ACCOUNTABILITY 137
V SMALL BUSINESSES 144
VI CALIFORNIA ONLINE PRIVACY PROTECTION ACT (2004) (CALOPPA) 145
(A) ORIGIN AND BACKGROUND 145
(B) PERSONAL INFORMATION 146
(C) OPERATOR 146
(D) DATA PROTECTION PRINCIPLES 147
VII CALIFORNIA CONSUMER PRIVACY PROTECTION ACT (2018) (CCPA) 149
(A) ORIGIN AND BACKGROUND 149
(B) PERSONAL INFORMATION 150
(C) BUSINESS 154
(D) DATA PROTECTION PRINCIPLES 159

VIII CONCLUSION *161*
CHAPTER 5 162
EU DATA PROTECTION LAW *162*
I INTRODUCTION *162*
II THE GENERAL DATA PROTECTION REGULATION (2016) (GDPR) *162*
(A) ORIGIN AND BACKGROUND *162*
(B) PERSONAL INFORMATION *163*
(C) CONTROLLER *169*
(D) DATA PROTECTION PRINCIPLES *175*
(I) CONSENT *178*
(II) OTHER GROUNDS OF LAWFUL PROCESSING *183*
(III) NOTICE *185*
(E) APPLICATION TO THE STUDY *187*
(F) DATA MINIMISATION *190*
(G) ACCOUNTABILITY *192*
III STATUTORY FRAMEWORK FOR E-PRIVACY *199*
IV CONCLUSION *218*
CHAPTER 6 220
SA DATA PROTECTION LAW *220*
I INTRODUCTION *220*
II SOUTH AFRICA'S APPROACH TO DATA PROTECTION *220*
III THE RIGHT TO PRIVACY UNDER SOUTH AFRICAN LAW *221*
IV THE PROTECTION OF PERSONAL INFORMATION ACT (2013) (POPIA) *222*
V ACCOUNTABILITY *252*
VI DATA MINIMISATION *257*
VII THE SUPPORTING STATUTORY FRAMEWORK FOR E-PRIVACY *259*
VIII AN ACCOUNTABILITY GAP? *268*
IX CONCLUSION *269*
CHAPTER 7 271
THE INCLUSION OF 'PRIVACY BY DESIGN' IN REGULATORY GUIDELINES FOR MOBILE APP DEVELOPERS IN THE US *271*
I INTRODUCTION *271*
II THE FOUNDATIONAL PRINCIPLES OF PBD *272*
III PBD IN THE UNITED STATES *274*
IV THE FTC PRIVACY FRAMEWORK *275*
V CALIFORNIA ATTORNEY GENERAL GUIDELINES *286*
VI SELF-REGULATION IS INSUFFICIENT *290*

VII REGULATORY ENFORCEMENT ACTIONS AGAINST APP DEVELOPERS *294*
VIII REGULATORY ENFORCEMENT ACTION AGAINST YOUTUBE *301*
IX CLASS ACTION AGAINST ZOOM VIDEO COMMUNICATIONS INC *303*
X CONCLUSION *308*
CHAPTER 8 311
THE INCLUSION OF "PRIVACY BY DESIGN" IN THE EU GENERAL DATA PROTECTION REGULATION *311*
I INTRODUCTION *311*
II PBD IN THE EU BEFORE GDPR *311*
III BACKGROUND TO THE ADOPTION OF PBD INTO GDPR *314*
IV ARTICLE 25 OF GDPR *317*
V CRITIQUE OF ARTICLE 25 ..... *319*
VI ACCOUNTABILITY *322*
VII THE ACCOUNTABILITY GAP *327*
VIII CONCLUSION *331*
CHAPTER 9 332
A "PRIVACY BY DESIGN" APPROACH UNDER THE PROTECTION OF PERSONAL INFORMATION ACT *332*
I INTRODUCTION *332*
II A PBD APPROACH IMPLIED BY LEGISLATION *332*
III A RANGE OF REGULATORY ENFORCEMENT MEASURES *333*
IV PRIVACY BY DESIGN APPROACH IMPLIED UNDER POPIA *336*
V A PROACTIVE AND PREVENTATIVE APPROACH *336*
VI PRIVACY AS THE DEFAULT *338*
VII PRIVACY EMBEDDED INTO DESIGN *342*
VIII FULL FUNCTIONALITY – POSITIVE SUM, NOT ZERO SUM *343*
IX END-TO-END LIFECYCLE PROTECTION *343*
X VISIBILITY AND TRANSPARENCY *344*
XI RESPECT FOR USER PRIVACY *345*
XII PRACTICAL APPROACHES TO PRIVACY BY DESIGN *345*
XIII CONCLUSION *348*
CHAPTER 10 349
CONCLUSION *349*
I INTRODUCTION *349*
II SUMMARY OF CHAPTERS *350*
III COMPARATIVE CONCLUSIONS *351*
IV PROPOSED AMENDMENTS *361*

V RECOMMENDATIONS FOR FUTURE RESEARCH *367*
VI CONCLUDING REMARKS *370*
TABLE OF LEGISLATION 372
INTERNATIONAL INSTRUMENTS *372*
UNITED NATIONS *372*
AFRICA *372*
COUNCIL OF EUROPE *372*
EUROPEAN UNION *372*
UNITED STATES *372*
STATE OF CALIFORNIA *375*
EUROPEAN UNION *375*
BELGIUM *378*
GERMANY *378*
UNITED KINGDOM *378*
SOUTH AFRICA *378*
AUSTRALIA *379*
CANADA *379*
HONG KONG *379*
TABLE OF CASES 380
SOUTH AFRICA *380*
UNITED STATES *381*
ZIPPO MANUFACTURING CO V ZIPPO DOT COM INC 952 F. SUPP. 1119 (W.D. PA. 1997) *383*
EUROPEAN UNION *383*
GERMANY *385*
BIBLIOGRAPHY 386
BOOKS *386*
CONFERENCE PAPERS AND CONFERENCE PROCEEDINGS *388*
NEWSPAPER ARTICLES *397*
COMMAND PAPERS, GUIDELINES, REPORTS AND INDUSTRY STANDARDS *398*
COUNCIL OF EUROPE *398*
COUNCIL OF THE EUROPEAN UNION *399*
EAST AFRICAN COMMUNITY *399*
EUROPEAN COMMISSION *399*
EUROPEAN NETWORK AND INFORMATION SECURITY AGENCY (NOW EUROPEAN UNION ASSOCIATION FOR CYBERSECURITY) *399*
INDUSTRY ASSOCIATIONS, PROFESSIONAL BODIES AND PRIVACY WATCHDOGS *400*
INDUSTRY STANDARDS AND TECHNICAL SPECIFICATIONS *401*

INTERNATIONAL TELECOMMUNICATIONS UNION *403*
INTERNATIONAL WORKING GROUP ON DATA PROTECTION IN TELECOMMUNICATIONS *403*
ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT (OECD) *403*
SOUTH AFRICAN GOVERNMENT DEPARTMENTS *404*
SOUTH AFRICAN LAW REFORM COMMISSION *404*
STATE OF CALIFORNIA: OFFICE OF THE ATTORNEY GENERAL *405*
UNITED NATIONS *405*
UNITED STATES FEDERAL GOVERNMENT DEPARTMENTS *405*
UNITED STATES FEDERAL TRADE COMMISSION *406*
OTHER *406*
DATA PROTECTION AUTHORITY PUBLICATIONS *407*
CANADA *407*
EUROPE *409*
EUROPEAN DATA PROTECTION BOARD *411*
EUROPEAN DATA PROTECTION SUPERVISOR *411*
UNITED KINGDOM INFORMATION COMMISSIONER'S OFFICE *412*
OTHER *412*
DISSERTATIONS *413*
INTERNET SOURCES *414*

LIST OF ABBREVIATIONS

AAID	Android Advertising ID
AD	Advertisement (as in ad library or ad server or ad tech)
AI	Artificial Intelligence
APEC	Asia-Pacific Economic Cooperation
API	Application processing interface
App	Application
AU	African Union
BPMN	Business Process Model and Notation
BSSID	Basic service set identifier
CalECPA	California Electronic Communications Privacy Act of 2015, Cal. Pen. Code §1546
CalOPPA	California Online Privacy Protection Act of 2003, Cal. Bus. & Prof. Code §§ 22575-22579 (2004
CCPA	California Consumer Privacy Act of 2018, Cal. Civ. Code §§ 1798.100– 1798.199
CJEU	Court of Justice of the European Union
COE	Council of Europe
Convention 108	Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data
COPPA	Children's Online Privacy Protection Act of 1998, 15 U.S.C. §§ 6501–6506
COREPER	Committee of the Council of the European Union
CPA	Consumer Protection Act 68 of 2008
CPC	Cost per Click
CPM	Cost per Mile
CRM	Customer relationship management
CSLI	Cell site location information
DAA	Digital Advertising Alliance
Data Protection Directive 95/46/EC	Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (Data Protection Directive) OJ 1995 L 281/31, 23.11.1995
DTPS	Department of Telecommunications and Postal Services (South Africa)
EC	European Council
ECA	Electronic Communications Act 36 of 2005
ECTA	Electronic Communications and Transactions Act 25 of 2002
EDPB	European Data Protection Board
EDPS	European Data Protection Supervisor

EECC	Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing The European Electronic Communications Code (Recast) OJ L 321, 17.12.2018
EFF	Electronic Frontier Foundation
EME	Exempted Micro Enterprise
ENISA	European Network and Security Agency
EPIC	Electronic Privacy Information Center
e-Privacy Directive 2002/58/EC	Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector 2002/58/EC (e-Privacy Directive) OJ L 201/37, 31.7.2002
ESSID	Extended basic service set ID
EU	European Union
FERPA	Family Educational Rights and Privacy Act of 1974, 20 U.S.C. § 1232g; 34 C.F.R. §§ 99.1 - 99.8 (FERPA)
FIPPs	Fair information practice principles
FIPs	Fair Information Practices
Framework Directive	Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services OJ L 108, 24.4.2002
FISA	Foreign Intelligence Surveillance Act of 1978, 50 U.S.C. §§ 1801 – 1885c (2018)
FOIA, US	The Freedom of Information Act of 1966, 5 U.S.C. § 552 (2018)
FTC	Federal Trade Commission
FTCA	Federal Trade Commission Act of 1914, 15 U.S.C. §§ 41 - 58 (2018)
GDPR	General Data Protection Regulation: Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA OJ L 119, 4.5.2016
GLBA	Gramm-Leach-Bliley Act of 1999, Pub.L. No. 106–102, 113 Stat. 1338
GN	Government Notice
GG	Government Gazette
GPS	Global Positioning System
GSMA	GSM Association
HEW	US Department of Health, Education and Welfare
HIPAA	Health Insurance Portability and Accountability Act of 1996, Pub.L. No. 104–191, 110 Stat. 1936
HIV	Human Immunodeficiency Virus
IaaS	Infrastructure as a Service
IAB	Interactive Advertising Bureau

ICCPR	International Covenant on Civil and Political Rights (adopted 16 December 1966, entered into force 23 March 1976) 999 UNTS 171
ICTs	Information and communication technologies
IDFA	Apple ID for Advertisers
IIEE	Institute of Electrical and Electronics Engineers
ISPs	Internet Service Providers
IT	Information technology
ITU	International Telecommunication Union
LAN	Local area network
MAC address	Media Access Control address
mBaaS	Mobile back-end as a service
MNO	Mobile network operator
mobile app	Mobile application
NAI	Network Advertising Initiative
NISO	National Information Standards Organisation
NIST	National Institute of Standards and Technology
NSEA	National Small Enterprise Act 102 of 1996
NTIA	National Telecommunications and Information Administration, United States Department of Commerce
OECD	Organisation for Economic Cooperation and Development
OECD Guidelines	Organisation for Economic Co-operation and Development (OECD) Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data
OEMs	Original Equipment Manufacturers
OS	Operating system
OSN	Online Social Network
PaaS	Platform as a Service
PAIA	Promotion of Access to Information Act 2 of 2000
PbD	Privacy by Design
PDVs	Personal data vaults
PETs	Privacy-enhancing technologies
PII	Personally identifiable information
POPIA	Protection of Personal Information Act 4 of 2013
QSE	Qualifying Small Enterprise
RFA	Regulatory Flexibilty Act of 1980, 5 U.S.C. §601–612 (2018).
RICA	Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 of 2002
SaaS	Software as a Service
SAIS	South Association for Information Systems
SDK	Software development kit
SMMEs	Small, medium and micro sized enterprises

SADC	Southern African Development Community
SQL	Structured Query Language
SSAID	Android device ID
SSID	Service set ID
SSL	Secure Socket Layer
TERMITE	ITU Telecommunication Terminology Database
TB	Tuberculosis
TLS	Transport Layer Security
UDHR	Universal Declaration of Human Rights (adopted 10 December 1948 UNGA Res 217 A(III)
UDID	Unique device identifier
UI	User Interface
UN	United Nations
UNCTAD	United Nations Conference on Trade and Development
US	United States
UX	User Experience
VPNs	Virtual private networks
W3C	World Wide Web Consortium
Wi-Fi	Wireless internet
WLAN	Wireless network
XSS	Cross-Site Scripting

TABLE OF TABLES

TABLE 1 KEY DATA PROTECTION TERMINOLOGY 37

TABLE 2 FACEBOOK'S TARGETING PARAMETERS MADE AVAILABLE TO ADVERTISERS……...54

TABLE 3 THE SEVEN FOUNDATIONAL PRINCIPLES OF PBD…….....97

TABLE 4 MAPPING PBD TO DATA PROTECTION PRINCIPLES…….....99

TABLE 5 AN INDICATIVE EXAMPLE OF ASSESSING RISKS WITH REGARD TO LEGAL COMPLIANCE……..336

TABLE OF FIGURES

FIGURE 1 THE IN-APP ADVERTISING ECOSYSTEM, INCLUDING THE INFORMATION FLOW BETWEEN DIFFERENT PARTIES. 61

CHAPTER 1

INTRODUCTION

I THE FUTURE IS DATA-DRIVEN

The impact of computer technologies on the protection of personal information has been a concern since at least the late 1960s,[1] but the principles developed when the threat was first perceived are proving challenging to apply in a digitised world in which personal information has become commoditised in a manner scarcely foreseeable a decade ago, and probably unthinkable four decades ago.[2]

Increasingly, data is recognised as having a commercial value, akin to currency,[3] and in the realm of digital services, the payment for so-called 'free' services is the glut of data that can be harvested from and about individuals using the services. Exponential increases in processing power mean that data can be collected, stored and analysed on a scale hitherto unthinkable. This is the era of 'big data'.

The term 'big data' refers to 'high-volume, high-velocity and high-variety information assets' that are leveraged though advanced analytics to provide cost-effective, efficient, evidence-based and often automated decision making.[4] It is 'a broad term that covers a great number of data processing operations, some of which are already well-identified, while others are still unclear and many more are expected to be developed in the near future'.[5] Its central tenet is that big data may reveal novel and unexpected correlations and drive innovation. Some argue that this innovation brings great benefits and is thwarted by the core data protection

---

[1] Organisation for Economic Co-operation and Development (OECD), *Thirty Years After the OECD Privacy Guidelines* (2011) at 16.
[2] Ibid at 62.
[3] Ibid.
[4] Gartner IT Glossary, 'Definition of Big Data' <https://www.gartner.com/en/information-technology/glossary/big-data#:~:text=Big%20data%20is%20high%2Dvolume,decision%20making%2C%20and%20process%20automation.> accessed 1 August 2020. Also see Amir Gandomi and Murtaza Haider, 'Beyond the Hype: Big Data Concepts, Methods, and Analytics.' (2015) 35 (2) *International Journal of Information Management* 137–144 at 138 &140, and Beverley A. Townsend and Donrich W. Thaldar 'Navigating Uncharted Waters: Biobanks and Informational Privacy in South Africa.' (2019) 35 (4) *South African Journal on Human Rights* 329–350 at 331.
[5] Article 29 Data Protection Working Party, *Statement on the impact of the development of big data on the protection of individuals with regard to the processing of their personal data in the EU* (WP 221, 16 September 2014) at 3. See further the discussion in chapter 2.

principles,[6] which have largely remained unchanged since they were first expressed in the 1980s.[7] Despite differences in scope, language, implementation measures, underlying legal traditions and cultural or social values, international, regional and national data protection laws are in 'broad agreement' on these core data protection principles.[8]

In Europe, data protection is now governed by the General Data Protection Regulation (GDPR) (2016),[9] which became effective on 25 May 2018. GDPR replaces the Data Protection Directive (1995),[10] but the core data protection principles remain unchanged. In the United States (US) there is no federal data protection statute of general application.[11] The Children's Online Privacy Protection Act (COPPA) (1998) [12] is enforced by the Federal Trade Commission (FTC) in relation to the personal information of children under thirteen and the FTC has developed Fair Information Practices (FIPs) guidelines. In California the California Online Privacy Protection Act (CalOPPA)[13] has regulated the requirement of a privacy policy. In the wake of the Cambridge Analytica scandal, California promulgated the California Consumer Privacy Act (CCPA)[14] (2018), and in addition US firms can voluntarily adhere to

[6] Ibid.
[7] *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980) has been updated in 2013, but the data protection principles remain unchanged: OECD, *The OECD Privacy Framework* (2013) at 4. As to earlier national data protection legislation enacted in the 1970s see OECD, *Thirty Years After the OECD Privacy Guidelines* at 16–17.
[8] Anneliese Roos, 'Data Protection: Explaining the International Backdrop and Evaluating the Current South African Position' (2007) 124 *SALJ* 400–437 at 405.
[9] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA OJ L 119, 4.5.2016 (EU General Data Protection Regulation; GDPR).
[10] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (Data Protection Directive) OJ 1995 L 281/31, 23.11.1995.
[11] Developments in this area are expected, but presently privacy is regulated at State level (in some States, such as California) and under a variety of sector-specific laws. For a general overview see California Department of Justice, 'Privacy Laws' (2019) <https://oag.ca.gov/privacy/privacy-laws> accessed 12 September 2019.
[12] Children's Online Privacy Protection Act of 1998, 15 U.S.C. §§ 6501 - 6506 (2018) (COPPA).
[13] The Online Privacy Protection Act of 2003, Cal. Bus. & Prof. Code §§ 22575–22579 (2004).
[14] The California Consumer Privacy Act of 2018, Cal. Civ. Code §§ 1798.100 - 1798.199 (CCPA).

the Privacy-Shield framework[15] or standard contractual clauses[16] on data transfers between the US and the European Union (EU). In South Africa, data protection is regulated by the Protection of Personal Information Act (POPIA) (2013),[17] as it has now come into operation with effect from 1 July 2020, with a one-year grace period for full compliance.[18] While there are differences in the scope and wording of these instruments, which will be explored in this study, they are all essentially grounded in the same core data protection principles.[19]

The shortcomings in these core principles will be discussed in depth in the theis. For example, in the EU and South Africa, the principle of data minimisation requires that personal information is processed (which includes collection and storage of personal information) only 'if given the purpose for which it is processed, it is adequate, relevant and not excessive'.[20] This principle is the corollary of the principle of purpose limitation, which requires that personal information 'must be collected for a specific, explicitly defined and lawful purpose related to a function or activity of the responsible party [data controller]'[21] and that voluntary, informed and specific consent must be given (unless another ground of lawful

---

[15] US Department of Commerce, 'EU-U.S. Privacy Shield Framework Principles ' <https://www.privacyshield.gov/servlet/servlet.FileDownload?file=015t00000004qAg> accessed 1 September 2019; US Department of Commerce, 'Swiss-US Privacy Shield Framework' <https://www.trade.gov/td/services/odsi/swiss-us-privacyshield-framework.pdf> accessed 1 September 2019. The Privacy Shield framework replaces the earlier "Safe Harbour" framework, but has recently been struck down as failing to offer adequate protection for trans-Atlantic data transfers as personal information transferred to the US is subject to surveillance under s 702 of the Foreign Intelligence Surveillance Act of 1978, 50 U.S.C. §§ 1801–1885c (2018) (FISA). See *Shrems II"* (C-311/18) ECLI:EU:C:2020:559 para 180–181 and the earlier judgments (decided pursuant to Directive 95/46/EC) in *Schrems, Maximillian v Data Protection Commissioner* (C-362/14) ECLI:EU:C:2015:650, *Google (Territorial scope of de-referencing)* (C-507/17) ECLI: EU:C: 2019: 772 and *Planet49* (C-673/17) ECLI:EU:C:2019:801.

[16] See the further discussion in chapter 5.

[17] Protection of Personal Information Act 4 of 2013 (POPIA).

[18] In Proc. R21 of 2020 *GG* 43461 of 22 June 2020 the President announced the commencement of ss 2–38; ss 55–109; s 111; and s 114(1), (2) and (3) POPIA with effect from 1 July 2020. In terms of s 114(1). all processing must be brought into conformity with the Act within one year from that date. This is expected to educe a long awaited overhaul of online privacy. Previously, South African data controllers could voluntarily subscribe to the privacy principles set out in chapter VIII of the Electronic Communications and Transactions Act 25 of 2002 (ECTA)and had to provide details on their website of their security procedures and privacy policy when supplying goods or services to consumers by way of an electronic transaction. Sections 110 and 114(4) shall commence on 30 June 2021. The provisions establishing the Information Regulator in s 1, part A of chap 5, and ss 112 –113 came into operation on 11 April 2014 in terms of Proc. R25 of 2014 in *GG* 37544 of 11 April 2014.

[19] Explanatory memorandum on the objects of the Protection of Personal Information Bill, published in *GG* 32495 of 14 August 2009 at para 2.6.1. Also see: South African Law Reform Commission, *Project 124 'Privacy and data protection'* (2009) at 648.

[20] POPIA s 10. GDPR art 5(1)(c). The principle is expressed in similar terms in *The OECD Privacy Framework* and other international, regional and national data privacy legislation to be discussed later.

[21] POPIA s 13(1). GDPR art 5(1)(b). The term 'responsible party' used in POPIA is equivalent to the term data 'controller' used in art 4(7) of the ibid.

processing exists).[22] In the US, processing requires notice of the purpose and consent. On the contrary, in practice, digital data controllers are incentivised by the promise of future, potentially lucrative, discoveries to be gleaned from data to collect and store as much data as possible, and a fortiori it is impossible at the time of data collection to obtain user consent to the processing of personal information for an as yet unknown future purpose.

There is no simple dichotomy between innovation and privacy protection. Unduly restrictive regulation may stifle innovation, and compromise the potential that innovation holds for economic and social benefits for society, organisations and individuals.[23] But more extensive – and intensive – uses of data pose an increased privacy risk,[24] and threaten consumer trust in and their adoption of digital innovations.[25] The challenge for legislators, regulators and industry is thus to 'innovate responsibly'.[26] The delicate balance to be struck requires that legislation should protect the individual's privacy but permit, and even facilitate, the appropriate use of data by commercial entities and governments. [27] The focus of the study is whether there is an 'accountability gap' in the protection of personal information in the mobile applications ecosystem under POPIA in South Africa. A comparative analysis of COPPA, CalOPPA and the CCPA in the US, and GDPR in the EU is undertaken to inform the consideration of the need for statutory reform to strengthen accountability for data protection under a privacy by re-design approach.

II THE ADVENT OF MOBILE APPLICATIONS

While the digital revolution culminated in the development of the internet in the 1990s, it is the smartphone that has dramatically accelerated the adoption of information and

[22] Definition of consent in POPIA s 1 and GDPR art 4(11).
[23] OECD, *Thirty Years After the OECD Privacy Guidelines* at 11.
[24] Preamble to the OECD, *Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data* (C(80)58/FINAL, as amended on 11 July 2013 by C(2013)79, 2013).
[25] See, for example, the consumer studies cited by Office of the Australian Information Commissioner, *Mobile privacy: A better practice guide for mobile app developers* (2014) at 4.
[26] State of California Office of the Attorney General, *Privacy on the Go: Recommendations for the Mobile Ecosystem* (2013), foreword by Attorney General Kamala D. Harris, i.
[27] See generally the discussion of the South African Law Reform Commission on the objectives of POPIA.

communication technologies (ICTs) and ushered in a 'fourth industrial revolution',[28] which is characterised by ubiquitous, mobile internet, powerful sensors, artificial intelligence (AI) and machine learning.[29] In some areas of the world, entire generations of technology are being 'leap-frogged' as communities move from an era with limited, and unreliable, fixed-line communication networks, to an ubiquitous smartphone-enabled internet-connected digital world.[30] It is now known that there are more active cellular subscriptions than people on the planet, although there continue to be marked regional disparities in access to ICTs.[31] Growth of mobile-broadband subscriptions is higher than that of fixed-broadband subscriptions, and most people now live within range of a mobile-cellular network signal.[32] The changes have been rapid. In South Africa, three years ago, 89% of the population owned a cellular telephone but only 37% owned a smartphone. Today 94% of South Africans surveyed own a cellular telephone, and 60% own a smart phone.[33] Smartphone ownership in South Africa rises even further to 73% of respondents between the ages of 18 and 34.[34]

Mobile applications (apps) are a relatively new phenomenon enabled by the development of the smart phone. Mobile apps are software applications that are designed to operate on a mobile device[35] and capable of close interaction with the hardware and operating system (OS) of the device through an application processing interface (API).[36] Since their

[28] The term was coined in 2016 by Klaus Schwab, founder and executive chairman of the World Economic Forum. Klaus Schwab, 'The Fourth Industrial Revolution: what it means and how to respond' (*World Economic Forum*, 14 Jan 2016) <https://www.weforum.org/agenda/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond> accessed 24 July 2018.
[29] Klaus Schwab, *The Fourth Industrial Revolution* (Portfolio Penguin 2017).
[30] For the example of Kenya see H.E.J Mucheru, 'Using tech to 'leapfrog' Kenya's development challenges: H.E. Joseph Mucheru (interview) ' (International Telecommunications Union (ITU) Plenipotentiary Conference, Dubai, 29 October–16 November 2018).
[31] ITU, *Measuring the Information Society Report Executive Summary 2018* (2018) at 2.
[32] Ibid.
[33] Pew Research Center, *Smartphone Ownership is Growing Rapidly Around the World, but Not Always Equally* (February 2019) at 9. A 'smartphone' is able to run appications and connect to the internet in addition to the basic telephony and SMS messaging functions of an ordinary cellular telephone.
[34] Ibid at 6.
[35] The term 'mobile device' includes not only smartphones, but laptops, tablets, other handheld devices such as gaming consoles, and wearable devices such as smartwatches.
[36] Article 29 Data Protection Working Party at 4.

introduction a little over 10 years ago,[37] the use of mobile apps has expanded exponentially to the point where there were an estimated 194 billion app downloads in 2018.[38]

Mobile apps now feature in every conceivable facet of human life,[39] ranging from the comparatively trivial areas of gaming and entertainment, to social networking, health, lifestyle and finance apps[40] that have access to highly personal and sensitive information.[41] Additionally, app users are no longer passive data subjects, as mobile apps permit the creation and sharing of content which may include personal information about others.[42] For example, when users 'tag' others in social media posts and photos, they not only share personal information about the other person (usually without explicit consent) but also legally implicate that person by association with the content.[43]

Moreover, given the vast volumes of data available and advanced analytics capabilities, the advertising and analytics industries have developed new technologies to track users across devices and to analyse, predict and shape their behaviours and preferences, and monetise the personal information about them.[44]

III NEW RISKS TO PRIVACY

Regulators are beginning to address the implications of big data, including the legal and ethical issues raised by tracking technologies and behavioural profiling based on the personal

---

[37] The Apple app store launched in July 2008 with 500 apps and the Google Play store (then known as Android market) launched in October 2008.

[38] AppAnnie, 'The State of Mobile 2019' (2018) <https://www.appannie.com/en/go/state-of-mobile-2019/> accessed 15 May 2020. An underreported statistic is the percentage of apps that fail to successfully deploy or scale in such a highly competitive market.

[39] ibid; user's time spent in apps as a measure of engagement shows that the top three app categories are social and communication apps, video players and editors and games.

[40] The categorisation of apps in the App Store and the Google Play store is not identical. See Apple, 'Categories and Discoverability - App Store - App Developer' <https://developer.apple.com/app-store/categories/> accessed 16 May 2019. Also see Google, 'Select a category for your app or game' <https://support.google.com/googleplay/android-developer/answer/113475?hl=en> accessed 16 May 2019.

[41] What is categorised in non-legal literature as 'sensitive' data, and the labelling of permission requests for certain types of data such as user location as 'dangerous', is not necessarily analogous with the legal definition of 'personal' data and the legal categorisation of certain types of 'sensitive' data as 'special' categories of personal data. See POPIA s 1 & ss 26 – 33. Also see GDPR arts 4(1) and 9.

[42] *Thirty Years After the OECD Privacy Guidelines* at 62, discussing the challenge of attributing legal responsibility in a multi-party environment. While users of mobile apps often play an active role in creating and sharing content the term 'data subject', with its implication of a purely passive role, continues to be used in data privacy legislation. See e.g. POPIA s 1 and GDPR art 4(1).

[43] *H v W* 2013 (2) SA 530 (GSJ) and *Isparta v Richter and Another* 2013 (6) SA 529 (GNP). See further Anneliese Roos, 'Privacy in the Facebook Era: A South African Legal Perspective' (2012) 129 *SALJ* 375–402.

[44] *Thirty Years After the OECD Privacy Guidelines* at 31.

information collected.[45] The issue of user tracking and data sharing is particularly complex in the mobile ecosystem. In Europe, the Article 29 Working Party[46] highlighted the risks in its February 2013 opinion on apps on smart devices in which it recognised that apps can 'access significantly more data than a traditional internet browser'. [47]

It has been said in relation to data protection that a watched society is a conformist society.[48] Smartphones are the ultimate surveillance mechanism, recording vast quantities of personal information about their user's whereabouts, and online activities and preferences. Smartphones are enabled with sophisticated sensors capable of precise location tracking, audio and video recording capabilities and cameras, as well as storage of contacts, photographs, documents and other personal information.[49] All of the data generated by these sensors, as well as the ability to read and write data in contacts, calendars and other applications can be made available to a mobile app through the API of the smartphone's operating system (OS).[50]

Large quantities of personal information can be transferred from the device, often without the knowledge of the app user, to app developers (defined by Grundy and others as 'first parties') but also frequently to third parties, and even further shared to fourth parties.[51] The identities of those third parties and fourth parties and the purposes for which they will use the data is often not disclosed.[52] Grundy and others[53] found that typically third parties reserve

---

[45] Article 29 Data Protection Working Party, *Opinion 2/2010 on online behavioural advertising* (WP 171, 22 June 2010) at 6–7. Also see Article 29 Data Protection Working Party, *Statement on the impact of the development of big data on the protection of individuals with regard to the processing of their personal data in the EU*, European Data Protection Supervisor (EDPS), *Privacy and Competitiveness in the Age of Big Data: The Interplay between Data Protection, Competition Law and Consumer Protection in the Digital Economy* (2014) and European Data Protection Supervisor (EDPS), *Opinion 8/2016 on the Coherent Enforcement of Fundamental Rights in the Age of Big Data* (2016).

[46] This was an independent European advisory body on data protection and privacy established under Article 29 of Directive 95/46/EC. Its tasks were described in Article 30 of Directive 95/46/EC and Article 15 of Directive 2002/58/EC. It existed from 1997 to November 2016. A full archive of its opinions and investigations can be found at https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/index_en.htm. Accessed on 22 April 2019.

[47] Article 29 Data Protection Working Party, *Opinion 02/2013 on apps on smart devices* (WP 202, 27 February 2013) at 5.

[48] South African Law Reform Commission at 16.

[49] Article 29 Data Protection Working Party, *Opinion 02/2013 on apps on smart devices*.

[50] Ibid.

[51] Quinn Grundy and others, 'Data Sharing Practices of Medicines Related Apps and the Mobile Ecosystem: Traffic, Content, and Network Analysis' (2019) 364 *BMJ* 1920 at 5.

[52] Ibid at 5.

[53] Ibid.

the right to collect de-identified and aggregated data, to use that data for their own commercial purposes, to share that data with their commercial partners (fourth parties) and to retain ownership of the data and the right to transfer it as a business asset. Grundy and others classify third parties as infrastructure suppliers and analysis entities.[54]

Infrastructure suppliers,[55] such as cloud services, are typically engaged by developers to store or process data, and may provide data analytics for app optimisation but would probably not monetise the data through further fourth party sharing.[56] The introduction of third-party infrastructure suppliers poses an additional layer of security vulnerability, but remains a relatively low privacy risk, as they operate within the framework of a contract with the developer as client, and thus their processing of data 'likely does not involve commercialising app user data for third party purposes'.[57]

In the second category of entities, Grundy and others' study of health apps identified transfers to entities broadly classified as software and technology companies (55%), digital advertising agencies (33%), corporate vehicles owned by privacy equity/venture capital firms (8%), major telecommunications corporations (3%) and a consumer credit reporting agency (1%).[58] That those third parties will probably use the data for precisely targeted advertising, algorithmically derived decisions in relation to, for example, insurance premiums, or other financial and social services, or for their own (and their business partners') product enhancement and development was referred to in opaque terms such as 'integrations'[59] and 'monetisation practices'.[60]

---

[54] Ibid.

[55] Under this term Grundy and others (ibid at 5) includes the provider of the following types of service: cloud computing (e.g. Amazon Web Services and Microsoft Azure); content delivery networks (e.g. Amazon CloudFront, CloudFlare), managed cloud providers (e.g. Bulletproof, Rackspace, Tier 3), database platforms (e.g. MongoDB Cloud Services), and data storage centres (e.g. Google).

[56] Ibid at 5.

[57] Ibid at 5.

[58] Ibid at 7.

[59] Ibid at 6. Integrations allow developers to access and export data. This may be done to enhance user experience, e.g. links to social media accounts that allow users to share and post content. However, it is also used to monetise apps through advertising. Also see Narseo Vallina-Rodriguez and others, 'Tracking the trackers: Towards understanding the mobile advertising and tracking ecosystem' (1st Data and Algorithm Transparency Workshop, New York, NY, 2016); Reuben Binns and others, 'Third Party Tracking in the Mobile Ecosystem' in *Proceedings of the 10th ACM Conference on Web Science* (ACM, Amsterdam, Netherlands 27–30 May 2018).

[60] Ibid at 6. Some apps are paid apps or offer a 'freemium' service with a free basic version and paid plans or subscriptions for additional services. The majority of apps are 'free' to download but are monetised through in-app purchases, or through in-app advertising, or through selling of deidentified and aggregated data and analyses. See generally: Binns and others; Grundy and others; Vallina-Rodriguez and others and Tobias Dehling and others,

IV NATURE AND EXTENT OF THE RISK

These new risks undoubtedly raise privacy qualms at a general level, but to understand the legal nature and extent of the risk one must distinguish the terms 'privacy' from 'personal information' and 'data protection.' While privacy is notoriously difficult to define in the abstract,[61] it is used in this dissertation to refer to 'the ability of individuals to know how their personal information will be collected, shared and used, and to exercise choice and control over its use'.[62] The right to privacy recognised in South Africa[63] and the European Union,[64] and under binding international law,[65] is integral to the approach adopted in both South Africa and the European Union to the protection of personal information.[66] The position in the US is

---

'Exploring the Far Side of Mobile Health: Information Security and Privacy of Mobile Health Apps on iOS and Android' (2015) 3 *JMIR Mhealth Uhealth* at 8.

[61] *Bernstein and others v Bester and others NNO* 1996 (2) SA 751 (CC) para 64–65 cautions that privacy has been described as an 'amorphous' and 'elusive' concept, that can never be comprehensively defined in the abstract; in fact attempts to do so would be 'inadvisable' if not 'impossible'. For the existence of an expectation of privacy is heavily context dependent, and must thus be worked out, on a case by case basis.

[62] GSM Association (GSMA), *Privacy Design Guidelines for Mobile Application Development* (February 2012) at 3.

This echoes the classic formulation of privacy in Alan F. Westin, *Privacy and Freedom* (Athenum 1967) as the right of individuals 'to choose freely under what circumstances and to what extent they will expose themselves, their attitudes, and their behaviour to others'. For a discussion of the four states of privacy: solitude, anonymity, intimacy and reserve see Westin at 31–32.

[63] Constitution of the Republic of South Africa, 1996 s 14.

[64] The Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, ETS no. 005 open for signature 4 November 1950, entry into force 3 September 1953 art 8 and Charter of Fundamental Rights of The European Union (2000/C 364/01) art 7 both enshrine a right to respect for private and family life.

[65] Universal Declaration of Human Rights (adopted 10 December 1948 UNGA Res 217 A(III). Although South Africa abstained from the vote adopting the resolution, it is enjoined by virtue of its membership of the United Nations and in particular Articles 55 and 56 of the United Nations Charter to promote 'universal respect for, and observance of, human rights and fundamental freedoms for all without distinction as to race, sex, language or religion.' Also see International Covenant on Civil and Political Rights (adopted 16 December 1966, entered into force 23 March 1976) 999 UNTS 171 (ICCPR) and Convention on the Rights of the Child, adopted by General Assembly resolution 44/25 of 20 November 1989, entry into force 2 September 1990. The ICCPR was signed by South Africa in 1994 and ratified in 1998. The Convention on the Rights of the Child was signed by South Africa in 1993 and ratified in 1995. Status available at http://indicators.ohchr.org/; accessed on 29 August 2018.

[66] In South Africa, the purpose of POPIA is set out in the Preamble and section 2 is 'to give effect to the constitutional right to privacy', which includes the right to be protected against 'the unlawful collection, retention, dissemination and use of personal information.' POPIA followed the model of article 1(1) of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (Data Protection Directive) OJ 1995 L 281/31, 23.11.1995which read:

'In accordance with this Directive, Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data.'

complicated by the absence of a standalone right to privacy in the federal Constitution,[67] although a right to privacy has been introduced into the constitution of the State of California.[68] There are thus both legal and cultural differences in how privacy is protected in the three jurisdictions.[69] Moreover, the line between 'private' information and 'personal' information is murky and difficult to draw.

In South Africa, the Constitution of the Republic of South Africa, 1996 (the Constitution, 1996) protects the right to *privacy*, not the right to protection of *personal information*. This is an important distinction,[70] given the unprecedented concentration of data in the hands of governments and private corporations which control the means of technological

[67] In America there is no constitutional right to privacy but in relation to the powers of government a 'reasonable expectation of privacy' has come to be applied to the concept of a search in the 4th amendment protection against unreasonable searches and seizures. Although the term privacy is not used in the 4th Amendment, its object has been described as being to protect 'the privacies of life' against 'arbitrary power' *Boyd v United States* 116 U S 616, 630 (1886). Privacy protections are also implicit in the 1st amendment protection of freedom of speech, freedom of religion and freedom of association, the 3rd amendment which prohibits the stationing of troops in private homes during peacetime, and the 5th amendment protection against self-incrimination. The position is similar in Canada. See further the reference in *Bernstein v Bester* para 75, where it is pointed out that the American constitutional approach involves a single inquiry into whether a right has been violated, and not the two-stage analysis adopted in South Africa (and, for example, in Canada) of whether the right has been infringed, and whether the limitation is reasonable and justifiable. Cf the cautionary remarks in the minority judgment of Kriegler J para 132, concerning the dangers of drawing conclusions from apparent similarities.

[68] California Constitution.

[69] David H. Flaherty, *Protecting Privacy in Surveillance Societies: The Federal Republic of Germany, Sweden, France, Canada, and the United States* (The University of North Carolina Press 1989) at 373–374, records that European concern with data protection stems from the European experience in World War II where data files stored by government agencies were used by the Nazis to hunt down target populations. Also see at 24–25 his comparison of different approaches to data protection, contrasting in broad terms the specificity that is characteristic of civil law systems, and the particular legalism inherent in the West German approach, with the common law heritage inherent in the North American approach of enacting general legislation that acquires specificity from the manner in which it is implemented by the civil service (or it must be added or regulated through judicial oversight). South Africa has its own egregious colonial and apartheid history of systematic discrimination based upon the classification of persons into race groups, which renders automated profiling of individuals without adequate safeguards for the rights of dignity, equality, freedom and privacy, particularly repugnant.

[70] E.g. in *NM and others v Smith and others (Freedom of Expression Institute as amicus curiae)* 2007 (5) SA 250 (CC) is at pains to set out a test for 'private' facts [para 34] and the remarks tha 'private medical information, … is personal information, which is protected by the right to privacy' must be understood in this context. POPIA defines 'personal information' much more broadly. See generally: Fred H. Cate, 'The Failure of Fair Information Practice Principles ' in Jane K. Winn (ed), *Consumer Protection in the Age of the 'information Economy'* (Ashgate Publishing Limited 2006); David H. Flaherty, *Protecting Privacy in Surveillance Societies: The Federal Republic of Germany, Sweden, France, Canada, and the United States* (The University of North Carolina Press 1989), Anneliese Roos, 'The law of data (privacy) protection: a comparative and theoretical study' (2009); Anneliese Roos 'Data Protection' in Van der Merwe D (ed) *Information and Communications Technology Law* (2 ed, LexisNexis 2016), Yvonne Burns and Ahmore Burger-Smidt *A Commentary on the Protection of Personal Information Act* (LexisNexis 2018) and South African Law Reform Commission, *Project 124 'Privacy and data protection'* (2009).

surveillance.[71] This has led to the development of a right to the protection of personal information in the EU,[72] although data protection and privacy are closely linked,[73] and there remains scholarly debate about the distinction, if any, between a right to data protection and a right to information privacy.[74]

Nevertheless, in all three jurisdictions, it is acknowledged that ubiquitous tracking, profiling, data matching and targeted advertising is unquestionably an intrusion upon the personal sphere and an infringement of the right 'to be let alone';[75] that is, the right to enjoy the 'sphere of intimacy' to which each person is entitled.[76] Thus, such practices also threaten autonomy, the right to direct one's own mind and actions, which is a fundamental component of the right to human dignity.[77]

Studies show that the data collected from mobile apps becomes concentrated in the hands of a few tech 'giants', notably Google and Facebook.[78] Coupled with the fact that this facilitates aggregation of data across multiple devices or sources (using semi-persistent identifiers such as an Android ID), the data collected by smartphones through mobile apps

---

[71] For contemporary accounts from a broad socio-legal perspective see Michael Chertoff, *Exploding Data: Reclaiming Our Cyber Security in the Digital Age* (Atlantic Monthly Press 2018) and Shoshana Zuboff, *The Age of Surveillance Capitalism - The Fight for a Human Future at the New Frontier of Power* (Profile Books 2019). For an exploration of State surveillance in South Africa see Jane Duncan, *Stopping the Spies: Constructing and resisting the surveillance state in South Africa* (Wits University Press 2018).

[72] Charter of Fundamental Rights of The European Union (2000/C 364/01) art 8. This change is reflected in GDPR which records its purpose in art 1(2) in relation to the right to the protection of personal data in particular, but refers also to all fundamental rights and freedoms which would, of course, continue to include the right to privacy protected under art 7 of the Charter.

[73] *Google Spain SL and Google Inc* (C-131/12) ECLI:EU:C:2014:317 para 53 and *Puškár* (C-73/16) ECLI: EU:C:2017:725 para 38. Both cases were decided under Directive 95/46/EC.

[74] For a discussion of the origins and meaning of the right to data protection see Carl Van der Maelen, 'Digital Privacy Protection Against Corporate Actors in the European Union: Benefits, Flaws and Repercussions' (Masters thesis, Ghent University 2017). Also see Orla Lynksy 'Deconstructing data protection: the "added-value" of a right to data protection in the EU legal order' (2014) 63(3) *International and Comparative Law Quarterly* at 4-6. Lynsky argues that although the memorandum to the Charter fails to provide an adequate explanation of the rationale for and scope of the right to data protection in the EU, it is a *distinct* right from the right to privacy, although 'heavily overlapping'. This is a distinction not recognised in South Africa where the Constitution recognises data protection only in as much as it is a subset of the right to privacy.

[75] The phrase was first used by in the seminal essay on the right to privacy under American law by Samuel D. Warren and Louis D. Brandeis, 'The Right to Privacy' (1890) 4 *Harvard LR* 193–220.

[76] *Khumalo and others v Holomisa* 2002 (5) SA 401 (CC) at 419A.

[77] Ibid, held that there are no 'sharp lines' between the rights to privacy and dignity. As to the distinction, see the fuller discussion in chapter 2 of South African Law Reform Commission report.

[78] Binns and others at 5 and Grundy and others at 10.

creates a heightened threat to privacy.[79] Moreover, data can also be used for anti-competitive and discriminatory practices.[80]

App developers themselves are often presented with a lack of transparency and a 'take it or leave it' attitude from large service providers,[81] leaving no room for app developers to design apps that fulfil the requirement of being truly voluntary specific and informed consent to data sharing.

As a counter-point to the generally alarmist note sounded in academic literature, developer conversations highlight the potential benefits to society, organisations (including start-up app developers) and individuals that could flow from using data analytics to solve social problems[82] and to help start-ups achieve commercial success through better interaction with and understanding of their customer base.[83] Shilton and Greene argue that developer conversations may thus offer insight into the points in the development process and reasons that privacy becomes a concern for developers. [84] For example, a developer blog makes reference to privacy and security in the context of the need for a comprehensive data management strategy in order to automate and scale data analysis using AI and cloud computing.[85]

---

[79] Grundy and others at 10.

[80] Ibid at 2 & 9. Also see: Mary F.E. Ebeling, *Healthcare and Big Data: Digital Specters and Phantom Objects* (Palgrave Macmillan 2016) and Frank Pasquale, *The Black Box Society: The Secret Algorithms That Control Money and Information* (Harvard University Press 2015).

[81] Based on reports by South African small, medium and micro enterprises (SMMEs) developing mobile applications the terms of service must be accepted 'as is' to use the product or service. See Donnelly DL, 'Data Privacy in the Cloud: The Position of SMMEs Engaged in Mobile App Development in South Africa' in Singh U and others (eds), Global Trends in Management, IT and Governance in an e-World (E-MIG 2019 International) (CSSALL Publishers 2020). Many authors note that this is a widespread business model applied to digital products and services. See e.g. Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for businesses and policymakers* (March 2012) at 51).

.

[82] E.g. an app developed in South Africa offers free HIV-drug resistance screening and could potentially also address TB-drug resistance. Anne Gonschorek, 'Up in the Cloud - Hyrax Revolutionises Drug-Resistance-Testing' <https://www.offerzen.com/blog/up-in-the-cloud-hyrax-revolutionises-drug-resistance-testing> accessed 17 May 2019.

[83] E.g. Luno, a Bitcoin wallet and exchange developed in South Africa, but now based in Singapore, describes how it used data analytics to make critical business decisions. Anne Gonschorek, 'How Luno Uses Data to Make Product Decisions' <https://www.offerzen.com/blog/how-luno-uses-data-to-make-product-decisions> accessed 17 May 2019.

[84] Katie Shilton and Daniel Greene, 'Linking Platforms, Practices, and Developer Ethics: Levers for Privacy Discourse in Mobile Application Development' (2019) 155 *Journal of Business Ethics* 131–146.

[85] Dries Cronje, 'Quick guide to introducing AI to your company' <https://www.offerzen.com/blog/quick-guide-introducing-AI-to-your-company> accessed 17 May 2019. A search on 17 May 2019 by the researcher on the blog of Offerzen.com, the top developer recruitment site in South Africa, returned only four posts out of more

than 100 containing the word ‘privacy’. None of the articles specifically addressed data privacy issues; rather, privacy was ancillary to discussions about business strategy.

V LEGISLATIVE COMPLEXITY AND THE GOAL OF HARMONISATION

Despite broad agreement on eight core data protection principles in POPIA and GDPR, the framework of data protection legislation is inordinately complex. Although similar, the expression of the core data protection principles in GDPR and POPIA, and the FIPs underpinning COPPA and the CCPA, have some differences which will affect how they are to be interpreted and applied, and this creates an additional layer of complexity in the mobile applications ecosystem where:

1. legal compliance with the laws of multiple jurisdictions may be required;
2. the complex architecture of mobile applications typically involves one or more layers of data processing, and
3. cross-border data flows are common.

All of these complexities must now be contractually managed in a transparent manner.

In the EU, the proposed Regulation on Privacy and Electronic Communications (2017)[86] (hereinafter referred to as the e-Privacy regulation) is now expected to be enacted at the earliest in late 2020 and will repeal the Directive on Privacy and Electronic Communications (2002).[87] While the provisions of GDPR, and the data protection principles it espouses, apply with full force to mobile apps, the e-Privacy regulation contains additional specific rules pertaining to electronic communications data, which includes both the content and metadata processed by mobile apps.[88]

The spectre of overlapping, and inconsistent, legislative requirements and rules on cross-border transfers of data becomes unavoidable, as mobile apps often involve data flows to third parties

[86] Proposal for a regulation of the European Parliament and of the Council concerning the Respect for Private Life and the Protection of Personal Data in Electronic Communications and Repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) Brussels, 10.1.2017 COM(2017) 10 final 2017/0003 (COD).

[87] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector 2002/58/EC (e-Privacy Directive) OJ L 201/37, 31.7.2002.

[88] The interception of the content and metadata relating to communications is regulated in South Africa by the Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 of 2002 (RICA) (RICA).

in different jurisdictions from those of the app user and app developer.[89] GDPR provides for a rationalised 'one stop shop' enforcement structure, in the form of the European Data Protection Board (EDPB) as 'leading supervisory authority' for establishments within the EU carrying out cross-border transfers of data within the EU or to jurisdictions with adequate privacy safeguards.[90] However, member States may introduce specific national legislative requirements in addition to or in derogation from GDPR, as permitted. One example pertains specifically to processing the personal information of children, which is subject to additional protections.[91] The age of consent under GDPR is 16 years, but member states can impose a lower age (not below 13 years) by way of national legislation.[92] Under POPIA, the age of consent is 18.[93] In the US, app developers must comply with COPPA, which imposes a consent age of 13.[94]

Furthermore, GDPR has global reach through its extra-territorial scope.[95] A South African app developer whose app processes personal information of EU residents, either to offer them goods and services (even if free) or to monitor their behaviour,[96] must comply with GDPR. However, they may face multiple investigations by the data protection authorities of the various EU member states without the protection of article 56 where they have no 'establishment' in the EU.[97] Similar extra-territoriality provisions apply under COPPA and the CCPA if a South African app developer processes information pertaining to children in the US and consumers in California respectively. Moreover, they would also have to comply with POPIA, as this applies when personal information is 'entered in a record by or for a responsible

[89] GDPR chapter V; POPIA chapter 9. Apps with transfer data to jurisdictions that do not offer adequate privacy protections are subject to more stringent disclosure requirements and must obtain 'explicit' consent for the transfer. GDPR art 49(1)(a); cf POPIA s 72(1)(b), which refers simply to 'consent', raising questions about whether GDPR imposes a different and more stringent consent standard. Note that the more stringent standard may need to be complied with in any event: ibid s 3(2)(b).
[90] GDPR arts 56 and 60.
[91] Ibid art 8, read with recitals 38, 58, 65, 71 and art 6(1)(f); POPIA ss 34 & 35.
[92] GDPR art 8(1).
[93] POPIA s 1, definition of 'child'.
[94] COPPA. The analysis of COPPA's provisions and discussion of illustrative examples of enforcement actions under COPPA necessarily refers to children in this context but children per se are not the focus of this study.
[95] GDPR art 3(2).
[96] Ibid.
[97] European Data Protection Board, *Guidelines 3/2018 on the Territorial Scope of the GDPR (Article 3) - Version for Public Consultation* (16 November 2018) at 12.

party', either if that responsible party is domiciled in South Africa,[98] or if it 'makes use of automated or non-automated means' of processing the data in South Africa.[99] The provisions of POPIA apply to the exclusion of any 'inconsistent' legislation,[100] but where other legislation has 'more extensive provisions', those will prevail.[101]

VI PRIVACY BY DESIGN AS A HARMONISING PRINCIPLE: A LITERATURE REVIEW

This dissertation adopts the conceptual framework of 'Privacy by Design' (PbD), which is the 'concept of engineering privacy directly into the design of new technologies, business practices and networked infrastructure, in order to achieve the doubly-enabled pairing of functionality and privacy'.[102]

The concept of privacy by design encompasses seven foundational principles that were developed in the 1990s primarily as a means of aligning legal data protection principles with the technological goals of system developers.[103] The concept origintes from a 1995 joint report of the Canadian and Dutch data protection authorities,[104] although the term itself was coined later by Dr Ann Cavoukian.[105]

Privacy by design requires developers to be proactive about protecting privacy rather than reactive to data breaches.[106] Privacy must be the default setting. Privacy must be

---

[98] POPIA s 3(1)(a). This requirement is met if the app developer is a registered South African company. Where two or more entities are jointly regarded as responsible parties, potentially, they are subject to inconsistent or overlapping regulatory oversight.

[99] Ibid s 3(1)(b) read with s 3(4) defining 'automated means'. The section does not explicitly address the common situation in the mobile environment where processing occurs partly in South Africa (on the device of a South African resident, or on locally hosted servers) and partly in a foreign jurisdiction through third party service providers and cloud services located in other jurisdictions.

[100] Ibid s 3(2)(a). Note that the section does not expressly provide for extra-territorial application and could thus be interpreted to apply only to inconsistent domestic legislation, leaving courts to apply conflict of laws principles to determine whether POPIA or GDPR should govern the dispute.

[101] Ibid s 3(2)(b).

[102] A Cavoukian and M Prosch, *The Roadmap for Privacy by Design in Mobile Communications: A Practical Tool For Developers, Service Providers, and Users* (Toronto, ON, Canada: Office of the Privacy Commissioner, Ontario, Canada, 2010) at 3.

[103] Cavoukian, 'Privacy by Design The 7 Foundational Principles Implementation and Mapping of Fair Information Practices'at 2.

[104] Information and Privacy Commissioner Ontario Canada and Registratiekamer The Netherlands, *Privacy-Enhancing Technologies: The Path to Anonymity (volume 1)* (1995).

[105] Cavoukian A, Privacy by Design The 7 Foundational Principles (Information and Privacy Commissioner, Ontario, Canada, 2009, revised January 2011). The earlier 1995 report used a closely related term 'Privacy Enhancing Technologies' (PET).

[106] Cavoukian (2010) op cit note 119at 2.

embedded into the design of the technology. [107] Full functionality of the technology must not be compromised by privacy settings.[108] Security measures must protect the full data lifecycle.[109] There must be visibility and transparency about data practices, and user privacy must be respected.[110]

It is important to recognise that although privacy by design is not explicitly referred to in data privacy legislation (with the notable exception of article 25 of GDPR), it has achieved universal acceptance as the guiding philosophy underpinning data protection laws. In 2010, the 32nd International Conference of Data Protection and Privacy Commissioners adopted a unanimous resolution on PbD,[111] and the concept has continued to grow in popularity.[112]

Privacy by design is appropriate to the present study as a mobile app developers must be guided on how to implement existing, complex data protection laws in the development of mobile apps, but they cannot effectively do this alone. Cavoukian's work on mapping PbD to the fair information principles (FIPs),[113] and her work with Marilyn Prosch of the Arizona State University (ASU) Privacy by Design Lab's study on mobile technologies[114] are central to the present study and are discussed in chapters 3 and 7. Also central is the work on the application of PbD principles to the *redesign* of existing technolgies and systems - termed

---

[107] Ibid at 2–3.
[108] Ibid at 3–4.
[109] Ibid at 4.
[110] Ibid at 4–5. Also see A Cavoukian, *Privacy by Design and the Emerging Personal Data Ecosystem* (Toronto, ON, Canada: Office of the Privacy Commissioner, Ontario, Canada, 2012) at 16.
[111] *Resolution on Privacy by Design* (Jerusalem, 29 October 2010). See also A Cavoukian, *Privacy by Design Strong Privacy Protection – Now, and Well into the Future a Report on the State of PbD to 33rd International Conference of Data Protection and Privacy Commissioners* (Toronto, ON, Canada: Office of the Privacy Commissioner, Ontario, Canada, 2011) at 6 and A Cavoukian, *Privacy by Design in Law, Policy and Practice A White Paper for Regulators, Decision-makers and Policy-makers* (Information and Privacy Commissioner, Ontario, Canada, 2011).
[112] Kirsten Martin and Katie Shilton, 'Putting Mobile Application Privacy in Context: An Empirical Study of User Privacy Expectations For Mobile Devices' (2016) 32 *The Information Society* 200–216 at 201.
[113] Cavoukian A, Privacy by Design The 7 Foundational Principles Implementation and Mapping of Fair Information Practices (Information and Privacy Commissioner, Ontario, Canada, 2010). Also see A Cavoukian, 'Privacy by Design: Origins, Meaning, and Prospects for Assuring Privacy and Trust in the Information Era' in George O.M. Yee (ed), *Privacy Protection Measures and Technologies in Business Organizations: Aspects and Standards* (Aptus Research Solutions Inc. and Carleton University, Canada 2012).
[114] Cavoukian A and Prosch M, The Roadmap for Privacy by Design in Mobile Communications: A Practical Tool For Developers, Service Providers, and Users (Toronto, ON, Canada: Office of the Privacy Commissioner, Ontario, Canada, 2010).

Privacy by (re) Design (Pb(re)D).[115] While Pb(re)D can be applied by a single organisation to the redesign of legacy systems, Cavoukian and Prosch's work on the mobile eco-system pertinently identifies the need for all role players at all stages of the data lifecyle to take responsibility for data protection.[116] Likewise, a metastudy which provided important guidance on the development of a PbD approach to mobile app development,[117] concluded that:

> 'the influence of app developers is often limited and, to a great extent, the rules of the ecosystem are determined by industry stakeholders, such as platform providers. For a comprehensive approach in protecting privacy and data protection for mobile app users, these overarching issues of governance must not be neglected.'[118]

Nevertheless scholarship on PbD in relation to software engineering has not focussed specifically on mobile apps.[119] Although a number of studies have focussed on

[115] See A Cavoukian and Claudiu Popa, *Privacy by ReDesign: A Practical Framework for Implementation* (Toronto, ON, Canada: Office of the Privacy Commissioner, Ontario, Canada, 2011) and A Cavoukian, *Privacy by Design in Law, Policy and Practice A White Paper for Regulators, Decision-makers and Policy-makers* (Information and Privacy Commissioner, Ontario, Canada, 2011).
[116] A Cavoukian and M Prosch at 3.
[117] ENISA, *Privacy and Data Protection in Mobile Applications: A Study on the App Development Ecosystem and the Technical Implementation of GDPR* (November 2017).
[118] Ibid at 62.
[119] Cavoukian A, Shapiro S and Cronk RJ, *Privacy Engineering: Proactively Embedding Privacy, by Design* (IPC, Ontario Canada, 2014); Diver L and Schafer B 'Opening the Black Box: Petri Nets and Privacy by Design' (2017) 31 (1) *International Review of Law, Computers & Technology* 68-90; ENISA, *Privacy and Data Protection by Design: From Policy to Engineering* (2014); ENISA, *Privacy by Design in Big Data: An Overview of Privacy by Design in the Era of Big Data Analytics* (2015); Senarath A and Arachchilage NAG, 'Understanding Software Developers' Approach Towards Implementing Data Minimization' *arXiv preprint arXiv:180801479;* Senarath A and Arachchilage NAG, 'A Data Minimization Model For Embedding Privacy Into Software Systems' (2019) 87 (101605) *Computers & Security* 1-17 and
Van Rest J and others, 'Designing Privacy-by-Design' [2014] *Privacy Technologies and Policy* 55.

privacy risks in the mobile ecosystem,[120] with several studies on mobile health apps,[121] they do not discuss PbD. A comprehensive literature review has revealed a dearth of scholarship on the implementation of PbD in relation to information system ecosystems in general, and third party processing in particular.[122] Kurtz and Semmann conclude that the lack of 'feasible, accepted designs and implementations for dealing with third parties is a major research gap.'[123] One work which does specificially consider PbD in the context of mobile app development on the Apple app store and Google play platforms,[124] underscores the need to move from viewing such platforms as 'neutral intermediaries' to recognising their role in shaping how app developers instantiate privacy rules through technical design contraints and policies

---

[120] Binns R and others, 'Third Party Tracking in the Mobile Ecosystem' in *Proceedings of the 10th ACM Conference on Web Science* (ACM, Amsterdam, Netherlands, 27-30 May 2018) 23 – 31; Chen T and others, 'Information Leakage Through Mobile Analytics Services' in *HotMobile'14: Proceedings of the 15th Workshop on Mobile Computing Systems and Applications* (ACM, Santa Barbara CA 26-27 February 2014) 1-6; Cortesi A and others, 'Datacentric Semantics for Verification of Privacy Policy Compliance by Mobile Applications' in *International Workshop on Verification, Model Checking, and Abstract Interpretation* (Springer 2015) 61-79; Liu X and others, 'Privacy Risk Analysis and Mitigation of Analytics Libraries in the Android Ecosystem' (2019) 19 (5) *IEEE Transactions on Mobile Computing* 1184-1199; Martin K and Shilton K, 'Putting Mobile Application Privacy in Context: An Empirical Study of User Privacy Expectations For Mobile Devices' (2016) 32 (3) *The Information Society* 200-216; Thomas, K and others, 'Distilling Privacy Requirements For Mobile Applications' in *Proceedings of the 36th International Conference on Software Engineering* (ACM, Hyderabad, India 31 May–7 June 2014);Vallina-Rodriguez N and others, 'Tracking the trackers: Towards understanding the mobile advertising and tracking ecosystem' (*1st Data and Algorithm Transparency Workshop*, New York, NY, 2016); Wang H and Guo Y, 'Understanding Third-Party Libraries in Mobile App Analysis' in *39th International Conference on Software Engineering Companion (ICSE-C)* (IEEE/ACM, Buenos Aires 20-28 May 2017); Williams E and Yerby J, 'Google and Facebook Data Retention and Location Tracking through Forensic Cloud Analysis' in South Association for Information Systems (SAIS) (ed), *SAIS 2019 Proceedings* (2019) and Zang H and Bolot J, 'Anonymization of Location Data Does Not Work: A Large-Scale Measurement Study' in *Proceedings of the 17th Annual International Conference on Mobile Computing and Networking* (ACM, Las Vegas 19-23 September 2011).

[121] Dehling T and others, 'Exploring the Far Side of Mobile Health: Information Security and Privacy of Mobile Health Apps on iOS and Android' (2015) 3 (1) *JMIR Mhealth Uhealth* e8; Grindrod K and others, 'Locking it Down: The Privacy and Security of Mobile Medication Apps' (2017) 150 (1) *Can Pharm J (Ott)* 60-66
Grundy Q and others; 'Data Sharing Practices of Medicines Related Apps and the Mobile Ecosystem: Traffic, Content, and Network Analysis' (2019) 364 *BMJ* 1920 and Huckvale K and others, 'Unaddressed Privacy Risks in Accredited Health and Wellness Apps: A Cross-Sectional Systematic Assessment' (2015) 13 *BMC Medicine* 214-227.

[122] Christian Kurtz and Martin Semmann, 'Privacy by Design to Comply with GDPR: A Review on Third-Party Data Processors' (Twenty-fourth Americas Conference on Information Systems, New Orleans, 2018) at 5.

[123] Ibid at 7.

[124] Shilton K and Greene D, 'Linking Platforms, Practices, and Developer Ethics: Levers for Privacy Discourse in Mobile Application Development' (2019) 155 (1) *Journal of Business Ethics* 131-146.

implemented by the platform.[125] The study does not , however, consider the legal principles of accountability or data minimisation as a mechanism for effectively implementing PbD.[126]

There is a growing body of *legal* scholarship on PbD in the EU[127] after the introduction of PbD in article 25 of the GDPR, and some legal scholarship in the US.[128] In South Africa there has been vigourous debate in the field of health research around the concept of informed consent,[129] but there is no body of scholarship on PbD and only only one small study considering PbD and the mobile app ecosystem.[130]

It is encouraging that PbD has been endorsed by regulators in both the US[131] and the EU,[132] and it is to be hoped that it will receive due consideration by the Information Regulator in South Africa. As it gains widespread acceptance PbD may act as a harmonising principle by offering a systematic approach to the practical implementation of data protection principles in the development and design of mobile technologies. As such, PbD may help to

---

[125] Ibid.

[126] In this regard see Kurtz C and others, 'The Unlikely Siblings in the GDPR Family: A Techno-Legal Analysis of Major Platforms in the Diffusion of Personal Data in Service Ecosystems' in *Proceedings of the 52nd Hawaii International Conference on System Sciences* (Scholar Space, Grand Waile, Maui 8-11 January 2019) 5059-5068 and Millard C, 'At this rate, everyone will be a [joint] controller of personal data!' (2019) 9 (4) *International Data Privacy Law* 217-219.

[127] See in particular Lee A Bygrave, 'Data Protection by Design and by Default: Deciphering the EU's Legislative Requirements' (2017) 4 *Oslo Law Review* 105–120; Hustinx P, 'Privacy by Design: Delivering the Promises' (2010) 3 (2) *Identity in the Information Society* 253-255; Jasmontaite L and others, 'Data Protection By Design and by Default: Framing Guiding Principles Into Legal Obligations in the GDPR' (2018) 4 *Eur Data Prot L Rev* 168-189; and Koops B and Leenes R 'Privacy Regulation Cannot Be Hardcoded: A Critical Comment on the 'Privacy by Design' Provision in Data Protection Law' (2014) 28 (2) *International Review of Law, Computers & Technology* 159-171.

[128] Ira S Rubinstein, 'Regulating Privacy by Design' (2011) 26 *Berkeley Tech LJ* 1409–1546
Katyal SK and Grinvald LC, 'Platform Law and the Brand Enterprise' (2017) 32 *Berkeley Tech LJ* 1135-1182; Ira S Rubinstein and Nathaniel Good, 'Privacy by Design: A Counterfactual Analysis of Google and Facebook Privacy Incidents' (2013) 28 *Berkeley Tech LJ* 1333–1414.

[129] Njotini MN, 'Preserving the Integrity of Medical-related Information – How "Informed" is Consent?' (2018) 21 (1) *Potchefstroom Electronic Law Journal* 1-20; Staunton C and others, 'Safeguarding the Future of Genomic Research in South Africa: Broad Consent and the Protection of Personal Information Act No. 4 of 2013' (2019) 109 (7) *South African Medical Journal* 468-470; Townsend BA and Thaldar DW, 'Navigating Uncharted Waters: Biobanks and Informational Privacy in South Africa' (2019) 35 (4) *South African Journal on Human Rights* 329-350.

[130] Donnelly DL, 'Data Privacy in the Cloud: The Position of SMMEs Engaged in Mobile App Development in South Africa' in Singh U and others (eds), *Global Trends in Management, IT and Governance in an e-World (E-MIG 2019 International)* (CSSALL Publishers 2020).

[131] See principally Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers* (March 2012) at 22, and the further discussion in chapter 7.

[132] See European Data Protection Supervisor (EDPS), *Opinion 5/2018 Preliminary Opinion on Privacy by Design* (2018) and Information Commissioner's Office (UK), *Privacy by Design* (2008), discussed in chapter 8.

bridge the divide between US and EU approaches to data protection, [133] and contested meanings of the right to privacy, and its relation to the protection of personal information online.[134]

VII REGULATORY APPROACHES TO PRIVACY BY DESIGN IN RELATION TO MOBILE APPS

Two regulatory approaches to PbD will be outlined. First there is the approach of issuing regulatory guidelines on PbD, in an effort to encourage and educate app developers on how to implement PbD principles when they develop apps. This 'educative' approach is complemented by the development of industry guidelines for 'self-regulation'. The second approach involves the use of legal action to enforce compliance with data proteciton laws. It is an over-generalisation to say that the US has favoured the first approach, while the EU has moved towards the second approach by adopting PbD as a legal obligation in article 25 of GDPR. As the examples below illustrate, in both jurisdictions a mix of approaches has been taken.

In line with the first approach, best practice guidelines on PbD for app developers have been published by regulators in Europe,[135] the United Kingdom,[136] Hong Kong,[137] Canada,[138] Australia[139] and the US at a federal[140] and at a state level.[141]

---

[133] For a description of the collision course precipitated by the introduction of the GDPR see Schwartz PM, 'The EU-US Privacy Collision: A Turn to Institutions and Procedures' (2012) 126 *Harv L Rev* 1966-2009. Also see Bygrave LA, *Data Privacy Law: An International Perspective* (Oxford Scholarship Online 2014).
[134] See further the discussion in chapter 3.
[135] Article 29 Data Protection Working Party, *Opinion 02/2013 on apps on smart devices*.
[136] Information Commissioner's Office [UK], *Privacy in Mobile Apps: Guidance for App Developers* (2013).
[137] Office of the Privacy Commissioner for Personal Data Hong Kong, *Personal data privacy protection: what mobile apps developers and their clients should know* (2012).
[138] Office of the Privacy Commissioner of Canada, *Seizing Opportunity: Good Privacy Practices for Developing Mobile Apps* (2012). Also see Office of the Privacy Commissioner of Canada, *Report on the 2010 Office of the Privacy Commissioner of Canada's Consultations on Online Tracking, Profiling and Targeting, and Cloud Computing* (2011) and Information and Privacy Commissioner Ontario Canada, *The Roadmap for Privacy by Design in Mobile Communications: A Practical Tool for Developers, Service Providers, and Users* (2010).
[139] Office of the Australian Information Commissioner, *Mobile privacy: A better practice guide for mobile app developers* (2014).
[140] Federal Trade Commission, *Mobile Privacy Disclosures Building Trust Through Transparency* (February 2013). Also see Federal Trade Commission, *Mobile Apps for Kids: Current Privacy Disclosures are Disappointing* (February 2012). Also see Federal Trade Commission, *Mobile Apps for Kids: Disclosures Still Not Making the Grade* (December 2012). Also see Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for businesses and policymakers* (March 2012).
[141] State of California Office of the Attorney General.

Although PbD moves beyond a 'notice and consent' model to one which requires strong 'privacy-friendly' default settings, it is nevertheless necessary to consider how mobile app developers obtain consent when users are requested to alter default settings to allow the collection or sharing of personal information. Specific guidelines on consent have been published as a best practice for mobile app developers, providing examples of how to obtain informed consent.[142] Informed consent must be preceded by disclosure of a specific, explicit and legitimate purpose.[143] Blanket acceptance of general privacy terms does not meet GDPR requirements[144] and, as will be argued in this dissertation, is also inadequate for compliance with POPIA.[145]

Guidelines issued by industry associations,[146] civil society organisations[147] and owners of app marketplaces[148] re-iterate the same principles. While the challenges of communicating privacy practices on a small mobile screen are widely acknowledged, industry recommendations still require that consent notifications be clear, prominent and delivered at an appropriate time.[149] Similarly, civil society organisations endorse the same principles. [150]

The advertising industry has worked on developing an ad-tracking icon for use in the mobile setting,[151] and has published self-regulatory guidelines specifically for the mobile

---

[142] National Telecommunications and Information Administration (NTIA) US Department of Commerce, *Short Form Notice Code of Conduct to Promote Transparency In Mobile App Practices* (2013 July 25).
[143] GDPR art 5(1)(b). The consent requirements under GDPR and POPIA will be compared later. It is argued that the consent required under POPIA cannot be regarded as informed and thus as a lawful basis for processing unless there has been disclosure of the purposes for which the data is collected.
[144] Article 29 Data Protection Working Party, *Guidelines on Consent under Regulation 2016/679* (WP 259, 28 November 2017).
[145] POPIA s 1 definition of consent as voluntary, specific and informed consent. The provisions for consent in the US under COPPA and the CCPA are markedly different from each other and in certain respects from the GDPR and POPIA.
[146] GSM Association (GSMA), *Mobile Privacy Principles: Promoting Consumer Privacy in the Mobile Ecosystem* (January 2011).
[147] Future of Privacy Forum and Center for Democracy and Technology, *Best Practices for Mobile Applications Developers* (December 2011).
[148] See Apple, 'App store review guidelines' (19 December 2018) <https://developer.apple.com/app-store/review/guidelines/#metadata/> accessed 16 May 2019. Also see Google, 'Privacy, Security, and Deception' <https://play.google.com/about/privacy-security-deception/personal-sensitive/> accessed 16 May 2019.
[149] GSMA, *Mobile Privacy Principles: Promoting Consumer Privacy in the Mobile Ecosystem*. The industry guidelines and best practice examples are thus consistent with the guidelines endorsed by data regulators referred to above notes 29 – 35.
[150] Future of Privacy Forum and Center for Democracy and Technology.
[151] The 'Your Ad Choices' icon was developed in 2014: Digital Advertising Alliance, *DAA Ad Marker Implementation Guidelines for Mobile* (2014).

apps ecosystem.[152] These build on earlier self-regulatory guidelines for the desktop environment[153] and have more recently been supplemented with guidelines covering tracking across devices[154] and political advertising.[155]

In its 2013 report on mobile disclosures, the US FTC noted that two companies were developing privacy policy generators and privacy badges for mobile apps, and endorsed such efforts as a means of developing standardised, layered privacy policy wording.[156] There are now a number of proprietary privacy policy generators and privacy seals/badges,[157] some of which offer free features,[158] as well as 'open-source' privacy policy generators made available by the developer community on an 'as is' basis.[159]

Research and development is also being focused on mechanisms to provide individuals with further control over their data such as virtual private networks (VPNs),[160] personal data vaults (PDVs),[161] and research into whether current disclosure practices are adequate to properly inform users.[162]

Despite these developments, the data-sharing practices within the mobile ecosystem are ubiquitous and not transparent,[163] and are certainly nowhere close to achieving 'privacy by design' and 'by default' in practice. A 2018 study of close to one million mobile apps demonstrated that over 60% were transmitting personal information to third parties,[164]

---

[152] Digital Advertising Alliance, *Application of Self-Regulatory Principles to the Mobile Environment* (2013). Also see Network Advertising Initiative (NAI), *2015 Update to the NAI Mobile Application Code* (2015).
[153] Digital Advertising Alliance, *Self-Regulatory Principles for Online Behavioural Advertising* (2009) and Digital Advertising Alliance, *Self-Regulatory Principles for Multi-Site Data* (2011).
[154] Digital Advertising Alliance, *Application of the DAA Principles of Transparency and Control to Data Used Across Devices* (2017).
[155] Digital Advertising Alliance, *Application of the Self-Regulatory Principles of Transparency & Accountability to Political Advertising* (2018).
[156] Federal Trade Commission, *Mobile Privacy Disclosures Building Trust Through Transparency* at 27.
[157] E.g. 'TRUSTe Assurance ' <https://www.trustarc.com/> accessed 16 May 2019.
[158] 'Free Privacy Policy Generator' <https://www.freeprivacypolicy.com/free-privacy-policy-generator.php> accessed 16 May 2019.
[159] E.g. a privacy policy and terms and conditions can be created using 'App Privacy Policy Generator' <https://app-privacy-policy-generator.firebaseapp.com/> accessed 16 May 2019.
[160] E.g. the privacy policy generator ('Privacy Choice') has shifted focus to customer control and now offers a VPN service ('Hide my Ass'); 'PrivacyChoice' <https://www.privacychoice.org> accessed 16 May 2019.
[161] Information and Privacy Commissioner Ontario Canada, *Privacy by Design and the Emerging Personal Data Ecosystem* (2012).
[162] Agostino Cortesi and others, 'Datacentric Semantics for Verification of Privacy Policy Compliance by Mobile Applications' in *International Workshop on Verification, Model Checking, and Abstract Interpretation* (Springer 2015). Also see Ehimare Okoyomon and others, 'On The Ridiculousness of Notice and Consent: Contradictions in App Privacy Policies' (The Workshop on Technology and Consumer Protection (ConPro '19), 2019).
[163] Grundy and others.
[164] Binns and others.

most of which was terminating with Alphabet and Facebook.[165] Another 2018 study showed that Facebook was informed every time an app built with its software development kit (SDK) was installed, and received data about each time it was opened and for how long.[166] Additionally, many apps were sharing much more detailed personal information such as detailed travel information and personal data of passengers.[167] In a separate study, Facebook was found to be sharing user data with fourth-party data brokers for targeting advertising.[168]

Despite facilitating widespread data-sharing practices, several studies have concluded that developers routinely fail to provide adequate privacy disclosures,[169] and lack adequate understanding of relative risk for users.[170] Where mobile app privacy policies exist and disclose third party data sharing, one study found that they typically do no more than state that the use of data by third parties is subject to that third party's terms and conditions.[171] Third-party privacy policies, on the other hand, define their contractual relationship as being with the developer and refer app users back to the app developer.[172]

Although most regulatory efforts to date have been directed at education, regulators in both the US and the EU have increasingly brought enforcement actions against app developers for breach of existing data protection laws. For example, in the US the 'Brightest Flashlight App' faced charges by the FTC for failing to disclose to users that it shared personal information including precise location and Android ID with third-party advertisers. The app deceived users by offering a choice not to share data when in fact data was always

---

[165] Ibid.
[166] Privacy International, *How Apps on Android Share Data with Facebook (even if you don't have a Facebook account)* (2018).
[167] Ibid.
[168] Grundy and others at 6.
[169] Ibid. Also see: Achilleas Papageorgiou and others, 'Security and Privacy Analysis of Mobile Health Applications: The Alarming State of Practice' (2018) 6 *IEEE Access* 9390–9403; SR Blenner and others, 'Privacy Policies of Android Diabetes Apps and Sharing of Health Information' (2016) 315 *JAMA* 1051–1052; Kit Huckvale and others, 'Unaddressed Privacy Risks in Accredited Health and Wellness Apps: A Cross-Sectional Systematic Assessment' (2015) 13 *BMC Medicine* 214–227; Kelly Grindrod and others, 'Locking it Down: The Privacy and Security of Mobile Medication Apps' (2017) 150 *Can Pharm J (Ott)* 60–66; Ali Sunyaev and others, 'Availability and Quality of Mobile Health App Privacy Policies' (2015) 22 *Journal of the American Medical Informatics Association* 1–4.
[170] Max Van Kleek and others, 'Better the Devil You Know: Exposing the Data Sharing Practices of Smartphone Apps' in *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems* (CHI, Denver, Colarado 6–11 May 2017).
[171] Grundy and others at 6. The policy may name the third party and provide a link to their terms and conditions, but this is not always the case.
[172] Ibid.

automatically shared.[173] More recently Musical.ly was issued with a record fine as part of a settlement with the FTC for breaches of COPPA in relation to the 'TikTok' app[174] and in March 2020 Zoom Video Communications Inc, owner of the Zoom app, was cited in a civil class action for breaches of the CCPA.[175]

The Court of Justice of the European Union (CJEU) held the host of a Facebook fan page jointly responsible as a data controller along with Facebook for processing the data of visitors to the fan page. The processing took place without consent in the case of visitors to the fan page who did not have a Facebook account and had not consented to Facebook's terms of use for processing their personal information.[176] The court held that 'controller' must be given a broad interpretation.[177] While merely using the Facebook platform will not make a user a 'controller', the creator of a fan page selected the demographic criteria according to which Facebook would process the data of visitors to the page. It thus participated in determining the means and purpose of processing and was a joint controller.[178] However, the Court emphasised that joint responsibility as joint controllers does not imply 'equal' responsibility.[179] The level of responsibility would be determined in accordance with the individual circumstances of each case, such as the stage of processing and different degrees of processing in which each party participated.[180] The findings have recently been held to apply to the operator of a website that had embedded third-party content (namely the Facebook 'like' button) onto its website.[181] The same result would likely apply by analogy to the app developer in relation to a mobile app integrating third-party trackers.

---

[173] *In the matter of Goldenshores Technologies, LLC and Erik M. Geidl* FTC Dkt No C-4446 (Apr 9, 2014) (consent order).
[174] Lesley Fair 'Largest FTC COPPA settlement requires Musical.ly to change its tune' (27 Feb 2019). Available at https://www.ftc.gov/news-events/blogs/business-blog/2019/02/largest-ftc-coppa-settlement-requires-musically-change-its accessed on 29 August 2019.
[175] *Robert Cullen, individually and on behalf of all others v Zoom Video Communications Inc.* Case No 5:20-cv-02155 (ND Cal, Mar 30, 2020).
[176] *Wirtschaftsakademie Schleswig-Holstein* (C-210/16) ECLI:EU:C:2018:388. The case was decided under Directive 95/46/EC, but the definition of controller in GDPR is in all material respects identical.
[177] Ibid para 27–28, referring to *Google Spain SL and Google Inc* (C-131/12) ECLI:EU:C:2014:317 para 34.
[178] Ibid para 38–39. This was the case even though Facebook alone received and stored the personal information, and only shared aggregated user statistics with the host of the fan page.
[179] Ibid para 43.
[180] Ibid.
[181] *Fashion ID GmbH & Co. KG v Verbraucherzentrale NRW eV* (C-40/17) ECLI:EU:C:2019:629 para 75–76.

It thus seems likely that regulators will begin investigating mobile apps more closely and bringing enforcement actions for non-compliance with data protection laws.[182] This raises the question of how regulators will approach small app developers, who build their apps on third-party platforms.

VIII STUDY RATIONALE

New technologies such as mobile apps offer South African consumers and businesses unprecedented advantages in efficiency and innovation, and promise economic growth in the ICT sector, but there is a dark side. A lack of adequate protection for privacy and security of personal information may lower consumer trust in ICT and their adoption of new technology, while at the same time increasing the prevalence of cybercrime.

This study was also sparked by the considerations applied to small app developers. The study examines the application of data protection laws in the selected jurisdictions to mobile apps in general, and the findings of the study apply to all mobile app developers, large or small. However, in all three jurisdictions there is a concern with whether data protection laws will have a disproportionate impact upon small businesses, and in the context of South Africa it is especially important to ensure that small app developers can meaningfully participate in the ICT sector. South Africa's ICT policy framework[183] seeks both to promote the adoption of ICT and to ensure that small, medium and micro enterprises

---

[182] Richard R Pell, 'Third-Party Data Collection and Consent in Mobile Applications' (16 January 2019) <https://info.dechert.com/10/11731/january-2019/2019-01-15-third-party-data-collection-and-consent-in-mobile-applications.asp?sid=e3e7d5f3-d44e-4edc-93d5-0e787cb84a28#> accessed 25 April 2019.

[183] Department of Telecommunications and Postal Services (DTPS), *National Integrated ICT Policy White Paper* (GN 1212 in *GG* 40325 of 3 October 2016); DTPS, *Electronic Communications and Transactions Act (25/2002):*, *National e-Strategy Digital Society South Africa* (GN 887 in *GG* 41242 of 10 November 2017); DTPS, *Electronic Communications and Transactions Act (25/2002): National e-Government Strategy and Roadmap* (GN 341 in *GG* 40772 of 7 April 2017) and DTPS, *Electronic Communications Act (36/2005): Final Information and Communication Technology Small, Medium and Micro-Enterprise Development Strategy (Final ICT SMME Development Strategy)* (GN 1252 in *GG* 41243 of 10 November 2017). For further discussion see IST-Africa, *Report on ICT Initiatives, Research and Innovation Priorities and Capacity in IST-Africa Partner Countries* (IST Africa-Consortium, October 2017).

(SMMEs)[184] can participate in the ICT sector.[185] The National Planning Commission pithily summarises these objectives as follows:

> *'ICT will continue to reduce spatial exclusion, enabling seamless participation by the majority in the global ICT system, not simply as users but as content developers and application innovators.'* [186]

However, there is a growing concern internationally,[187] and within South Africa,[188] that the rapid globalisation of the last decade made possible by the internet has created a 'digital divide' that entrenches rather than removes existing inequalities. The growing digital divide coupled with possible future advances in robotics and digital automation threaten to disrupt the balance of trade further by shifting production back to industrialised nations, as the need for unskilled and semi-skilled labour is reduced.[189] This context is making it

---

[184] The term is not uniformly defined and careful attention to the classification applied by studies is necessary for comparison. In the US a mobile app developer is a small business if it has fewer than 1 000 employees. In the EU an SME has fewer than 250 employees and the subcategory small enterprise has fewer than 50 employees (subject to annual turnover and asset value thresholds). In South Africa a mobile app developer is an SMME if it employs no more than 250 employees. The subcategories small and micro enterprise describe entities with no more than 50 or 10 employees respectively (subject to annual turnover thresholds). See: National Small Enterprise Act 102 of 1996 (NSEA) s 1 read with the schedule (recently updated by GN 399 in *GG* 42304 of 15 March 2019). Cf US Small Business Administration, 'Table of Size Standards' (19 August 2019) <https://www.sba.gov/document/support--table-size-standards> accessed 5 March 2020 and *Recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises* (C(2003) 1422, OJ L 124/36). Note: An SMME under the NSEA is not to be confused with the nomenclature of 'qualifying small enterprise' (QSE) and 'exempted micro enterprise' (EME) under DTPS, *The Amended Information and Communication Technology (ICT) Broad-Based Black Economic (B-BBEE) Sector Code* (GN 1381 in *GG* 40407 of 7 November 2016). Also note: The activities of a mobile app developer would predominantly fall within the category 'transport, storage and communications' in the Schedule to the NSEA. Following Statistics South Africa, *Standard Industrial Classification of All Economic Activities (SIC)* (7 edn, Stats SA 2012), some empirical research and government statistics would report the activity of mobile app developers under sub-class 58200 ('software publishing') under the new section J (information and communication) (introduced in 2012).

[185] DTPS, *Electronic Communications Act (36/2005): Final Information and Communication Technology Small, Medium and Micro-Enterprise Development Strategy (Final ICT SMME Development Strategy)*. Also see Department of the Presidency Republic of South Africa (National Planning Commission), *National Development Plan Vision for 2030* (2011) at 117.

[186] *National Development Plan 2030: Our Future – Make it Work* at 190.

[187] See e.g. United Nations Conference on Trade and Development (UNCTAD), 'Digital transformation for all: empowering entrepreneurs and small business (Audio recording of conference proceedings on 25 April 2017)' (*UNCTAD e-commerce week*, 24–28 April 2017) <http://unctad.org/en/conferences/e-week2017/Pages/MeetingDetails.aspx?meetingid=1318> accessed 10 May 2017 showcasing the UNCITAL e-Commerce for All initiative. Also see UNCTAD, *Data protection regulations and international data flows: Implications for trade and development* (2016).

[188] DTPS, *National Integrated ICT Policy White Paper* (GN 1212 in *GG* 40325 of 3 October 2016), ch 5.

[189] DTPS, *Electronic Communications and Transactions Act (25/2002), National e-Strategy Digital Society South Africa* (GN 887 in *GG* 41242 of 10 November 2017) at 603.

increasingly important to focus on technological innovation within the SMME sector, as SMMEs are regarded as key to economic growth.[190]

The present study is important because mobile apps are often developed by a single individual or a small group of individuals who lack resources and privacy and security expertise.[191] One study found that 82% of apps were developed by small organisations.[192] Typically, developers employ third-party software in the development of the app, but it is common for developers to lack a full understanding of what data is being collected by third parties.[193]

App developers are not in a position to control the design and deployment of a mobile app unilaterally. When developers work for a client, they work within constraints with regard to scope, cost and time imposed by the client. Even when developers own the app, they work within a complex ecosystem in which they frequently use third-party code, and they may not be in a position to determine how the code functions in sharing data with third parties.[194]

App stores, being the platforms on which apps are marketed, can play a role in educating developers about privacy issues and enforcing compliance with privacy regulations, but compliance with the contractual requirements for acceptance into the app store cannot be relied upon by developers as a measure of full legislative compliance.[195] Conversely, researchers Greene and Shilton now argue that focusing only on the app developer's responsibility for privacy in the app design ignores how platforms themselves shape the understanding of what 'privacy' means.[196]

Large platform providers such as Internet Service Providers (ISPs), Original Equipment Manufacturers (OEMs), Operating Systems (OS), browsers, and 'social media

---

[190] Ibid.
[191] European Union Agency For Network and Information Security (ENISA), *Privacy and Data Protection in Mobile Applications: A Study on the App Development Ecosystem and the Technical Implementation of GDPR* (November 2017) at 12.
[192] Ibid at 31. Also see Children's Online Privacy Protection Rule; Final Rule Amendments, FR 79(12) Part II (17 January 2013) at 4 000 estimated that 90% of businesses affected by the COPPA rule would be small entities. Their report refers to a figure of 500 employees (which applied before the US size standard was amended to 1 000 employees). The figure may very well now be higher.
[193] ENISA at 13.
[194] Ibid at 13 states that third party libraries are 'often proprietary and closed-source and cannot be easily analysed.'
[195] Ibid at 18.
[196] Daniel Greene and Katie Shilton, 'Platform Privacies: Governance, Collaboration, and the Different Meanings of "Privacy" in iOS and Android Development' (2018) 20 *New Media & Society* 1640–1657 at 1643.

giants' may seek to track app user data 'comprehensively'.[197] For example, even after GDPR became effective on 25 May 2018, the Facebook SDK continued to share user data from the moment the app was downloaded, despite developer complaints that this made it impossible to comply with GDPR as users had not yet activated permission settings.[198] Data brokers may seek to aggregate and sell user data. Advertisers seek to aggregate user data in order to place targeted advertising. Most apps available as free downloads are at least partly monetised through in-app advertising or by selling anonymised reports based on user data.

A PbD approach applied throughout the mobile apps ecosystem could resolve some of these issues by ensuring that the technology and platforms upon which mobile apps are built and marketed are designed in such a way that by default privacy is protected. A meta-study of the European Network and Information Security Agency (ENISA) revealed no studies that had surveyed types of developers and their working conditions,[199] and cited only one study considering how best to give recommendations to developers who are SMEs.[200] The report recommended further study in this area that it should be considered whether it is possible to give 'generic' recommendations to app developers on data privacy compliance, or whether these need to be tailored, and if so, within which parameters: size of the developer organisation, app domain, type of app, team structure and development methodology.[201] Empirical, multi-disciplinary research of this nature lies beyond the scope of this dissertation. Instead, one of the important prior research questions that this dissertation addresses is the legal question of whether POPIA requires a PbD approach at all.

IX STUDY HYPOTHESIS AND KEY RESEARCH QUESTIONS

The dissertation considers whether there is an 'accountability gap' within the legislation selected for comparative study in this dissertation by examining whether the legislation can be enforced against parties other than the app developer in the mobile app ecosystem, as it is

---

[197] Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for businesses and policymakers* at 14.
[198] Privacy International.
[199] ENISA at 31.
[200] Ibid at 58. See: European Network and Security Agency, *Guidelines for SMEs on the Security of Personal Data Processing* (2016).
[201] ENISA at 31.

theorised that only on this basis will the underlying technologies and architecture of mobile apps be changed to support a privacy by (re)design approach.

The study hypothesis builds on four key assumptions:

1. Mobile apps pose a significant privacy risk due to their huge potential for processing personal data.
2. The mobile app ecosystem is complex because the means and purpose(s) of processing personal data is determined by multiple role-players, and ubiquitous cross-border data flows trigger legal compliance obligations in multiple jurisdictions.
3. PbD is an important conceptual framework that can address the legal complexities that make it difficult to apply existing data protection laws in such a complex ecosystem effectively, but requires concrete application in a specific context for effective implementation.
4. If platform owners,[202] hardware manufacturers and third party software providers are not held sufficiently accountable under existing regulatory and contractual frameworks, app developers will be vulnerable to legal liability but will lack effective means to implement a PbD approach.[203]

The dissertation's hypothesis is that for a PbD approach to be implied as an obligation for a responsible party to comply with POPIA, the statutory provisions on accountability and data minimisation must be adequate to implement such an approach effectively in the mobile apps ecosystem. The key research questions to be addressed are:

1. What is meant by the mobile apps ecosystem?
    a. What is a mobile app?
    b. Who are the role-players in the mobile apps ecosystem?

[202] The term 'platform' refers to a range of hardware and software that can host a mobile app, including the operating system (OS), app stores, online social networks (OSNs), and cloud 'platform-as-a service' providers. These terms and the role played by the owners of these platforms is explained in chapter 2.
[203] Promoting participation by SMMEs in the ICT sector is a key national policy objective, but in reality, small developers who lack the technical and legal expertise to understand and implement PbD requirements may be excluded from the industry. App stores may refuse to list the app, or may take down a non-compliant app, and users may uninstall an app they do not trust.

c. What role do they play in processing personal information of app users?

2. What is meant by a PbD approach?
    a. What are the core principles of data protection law?
    b. What are the principles of the PbD approach?
    c. How is the principle of accountability related to PbD?
    d. How is the principle of data minimisation related to PbD?
    e. How is the concept of informed consent related to PbD?
    f. What is the nature of PbD? Is it a new legal principle?
    g. What is meant by privacy by (re)design?
3. Under COPPA, the CCPA, GDPR and POPIA respectively:
    a. What is protected as personal information?
    b. What persons are held accountable for data protection?
    c. What are the data protection principles applied to:
        i. Accountability?
        ii. Data minimisation?
        iii. Informed consent?
4. Can Pb(re)D be enforced through self-regulation?
5. Can Pb(re)D be enforced through a direct legal obligation?
6. Is a Pb(re)D approach implied for compliance with POPIA by a responsible party?

X METHODOLOGY

The dissertation is a doctrinal study that will present a comparative legal analysis of the application of EU, US and South African data-protection legislation to mobile app developers. A comparative analysis is appropriate when seeking new knowledge or insights and to shape legal reform. It is particularly necessary in a study of data privacy, where international harmonisation is desirable on cross-border data flows, and data privacy laws 'embody a set of broadly similar principles'.[204] It is also relevant that mobile apps are not geographically restricted.

[204] Anneliese Roos, 'The law of data (privacy) protection: a comparative and theoretical study' (2009) at 20–21.

GDPR has been selected for a detailed comparative study because it is the most recent and comprehensive privacy regulation instrument, it has wide extra-territorial application and applies to many South African mobile app developers, and there is extensive regulatory guidance and case law on data privacy in European law.

The US has been selected for study because of its position as the domicile of many of the world's technology 'giants' including dominant firms in the mobile app ecosystem, namely Google, Apple and Facebook. As the US does not have a federal privacy statute and a full comparison of the position in all US States is beyond the scope of this work, two of the most influential statutes in the US, COPPA and the CCPA, have been selected for comparison. Brief reference is made to CalOPPA in California and other relevant statutes at a federal level.[205]

Reference will be made where relevant to international and regional privacy frameworks, the laws of other selected countries and the Privacy-Shield to provide an overview of the global data privacy framework.

The examination of the data privacy laws adopts a legal positivist approach, appropriate to the analysis of legislation. It is grounded in the constitutional protection of the right to privacy and related rights, which underpins data protection laws in the EU, the US (specifically the state of California) and South Africa.

[205] Chapter 4 surveys the federal statutes that may impact upon mobile app development in the US. COPPA was selected for detailed study as its novel provisions offer a useful model for comparison with POPIA and the formulation of possible amendments. Moreover there is a significant body of literature, regualtory reports and regualatory enforcement actions available in relation to COPPA. The online privacy laws of the state of California were selected as tech companies situated in the US, and the state of California in particular, occupy a dominant position in relation to mobile app development.

XI CHAPTER BREAKDOWN

Chapter one sets the scene, describing the background, rationale and aims of the study.

Chapter two defines key terminology and discusses data processing practices used within the mobile applications ecosystem.

Chapter three examines the concept of privacy by design (PbD). It commences by defining core data protection principles in their international and regional context. It then discusses the seven foundational principles of PbD and how those principles relate to the data protection principles, and introduces the term privacy by (re)design.

Chapters four, five and six provide an in-depth analysis of selected issues in the data protection laws in the US, the EU and South Africa. The concepts of personal information, responsible party, consent, other grounds for lawful processing, and notice are explained, with reference to two data protection principles identified as central to a PbD approach: data minimisation and accountability. These chapters provide the necessary basis for considering the enforceability of a Pb(re)D approach under the data protection laws in those jurisdictions.

Chapter seven critically examines the PbD guidelines issued to mobile app developers in the US and the FTC's endorsement of privacy by design. It will further consider the FTC's approach to industry self-regulation in the context of how a Pb(re)D approach might be applied to the mobile applications ecosystem. The chapter provides a counterpoint to the EU approach.

Chapter eight provides a critical analysis of the implementation of Pb(re)D through the adoption of article 25 of GDPR which imposes an express duty on data controllers to ensure data protection by design and by default.

Chapter nine builds on the earlier chapters to offer a conclusion as to whether a Pb(re)D approach is required for compliance by a responsible party with POPIA and to summarise the elements of such an approach.

Chapter ten sets out the comparative conclusions of the study, makes recommendations for certain amendments to South African law, and also proposes themes for future research.

XII KEY TERMINOLOGY

In this dissertation, the term 'data protection' is used as a convenient shorthand expression drawn from scholarly literature for the legislation and principles that have been adopted to protect personal information in a variety of international, regional, national and voluntary frameworks. The term 'data privacy', while sometimes used interchangeably,[206] has mostly been avoided, as there is a distinction between protecting 'private' information and protecting 'personal' information.

The term 'personal information' has been used whenever it is intended to indicate that the information falls within the protective ambit of the legislation selected for study. The term 'data' has a wider meaning (explored further in chapter 2) and where used should be understood subject to that caution.

A number of 'terms of art' are used in data protection legislation that are central to this dissertation but which, while often defined in a similar manner, have been labelled differently in the three jurisdictions studied. In chapters addressing the law of a particular country or state, the terminology used in the applicable legislation is adopted. When quoting directly from scholarly literature, the terms used by the author are used, but, unless indicated to the contrary, should be understood as encompassing equivalent terms used in POPIA. Otherwise, for consistency, this dissertation adopts as far as possible terms that are used in POPIA, being the South African legislation that is central to this study. Those terms should be understood, unless the context indicates to the contrary, as encompassing equivalent terms used in the US and EU legislation.

For ease of reference Table 1 (at the end of this chapter) sets out key terminology, providing terms used in POPIA and their definitions. The table then indicates in the three columns to the right the equivalent terms and their location in GDPR, COPPA and the CCPA. The term 'operator', for example, is used under COPPA in the US to indicate the party operating a website or online service; in other words, the party primarily responsible for COPPA compliance. The 'operator' of a mobile app may engage one or more service providers

---

[206] See for example Lee Bygrave's use of the term 'data privacy' as a term to draw closer connections between the US and EU approach to data protection in *Data Privacy Law: An International Perspective* (Oxford Scholarship Online 2014), at 107-116. However I have avoided the term because as I explained earlier there is an important legal distinction between the information protected under the Constitutional right to privacy and the much wider concept of 'personal information' in POPIA.

to perform particular functions related to the operation of the app. However, in South Africa, the person primarily responsible for compliance with POPIA is referred to as a 'responsible party', and the term 'operator' refers to any other person undertaking processing on behalf of the responsible party, that is, a service provider. In GDPR the equivalent terms are data 'controller' and data 'processor'.

Secondly, while POPIA and GDPR are omnibus statutes that apply to the personal information of any data subject,[207] they include special provisions pertaining to the personal information of children.[208] In the US, COPPA applies specifically to the information of a child[209] or information which the child supplies about his or her parents.[210] Although the CCPA applies only to the information of a 'consumer',[211] this could include a minor child as consumer, or within the 'household'[212] or 'family'[213] of an adult consumer. However, the age of consent differs dramatically. In South Africa a 'child' is defined as a person under the age of eighteen years,[214] and thus lawful consent to processing personal data can be obtained in

---

[207] Both apply to all living, natural persons. Additionally, POPIA can apply to juristic persons. GDPR art 4(1) defines a 'data subject' as 'an identified or identifiable person' and rec 27 provides that GDPR does not apply to deceased persons. Likewise, under POPIA s 1, a 'data subject', read with the definition of 'personal information', includes 'an identifiable, living natural person'. POPIA will not disturb the protection of personal information of a person who has not been dead for more than 20 years contained in PAIA. However, under POPIA, a 'person' is defined to include both natural and juristic persons, and the definition of 'personal information' includes 'information relating to … where it is applicable, an identifiable, existing juristic person'.

[208] GDPR art 8 and POPIA ch 3 part C (ss 34 & 35).

[209] COPPA §6502(a)(1) prohibits the online collection of personal information from a child. It reads:
'(a) Acts prohibited
(1) In general
It is unlawful for an operator of a website or online service directed to children, or any operator that has actual knowledge that it is collecting personal information from a child, to collect personal information from a child in a manner that violates the regulations prescribed under subsection (b).'

[210] COPPA §6501(8). The COPPA Rule CFR §312.2(10) defines 'personal information' to include 'Information concerning the child or the parents of that child that the operator collects online from the child and combines with an identifier described in this definition.'

[211] CCPA §1798.140(g) '"Consumer" means a natural person who is a California resident, as defined in Section 17014 of Title 18 of the California Code of Regulations, as that section read on September 1, 2017, however identified, including by any unique identifier.'

[212] CCPA §1798.140 (o)(1) defines 'personal information' as 'information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household'. The term 'household' is not further defined.

[213] CCPA §1798.140 (x) defines a 'unique identifier' as 'a persistent identifier that can be used to recognize a consumer, a family, or a device that is linked to a consumer or family, over time and across different services, …'. This includes minor children living in the household with a custodial parent or guardian: 'For purposes of this subdivision, "family" means a custodial parent or guardian and any minor children over which the parent or guardian has custody.'

[214] POPIA s 1 '"Child" means a natural person under the age of 18 years who is not legally competent, without the assistance of a competent person, to take any action or decision in respect of any matter concerning him- or herself;'

respect of the processing of a child's personal information only from a 'competent person',[215] such as a parent or legal guardian.[216] In the EU the age of consent is sixteen,[217] but member States have the power to derogate from this and provide by law for a lower age of consent not below thirteen years.[218] In the US, the age of consent is thirteen.[219] The protections available to children, although differing in their detail, thus apply uniformly to children twelve years old or younger. But children between twelve and eighteen, who may be most vulnerable to dangers of online stalking, sexual grooming, trafficking and cyber-bullying, may have no special protection in certain jurisdictions.

Although 'accountability' is not included in the legislative terms of art defined in table 1 it is a term central to the hypothesis that there is an 'accountability gap' in the legislation selected for comparative study. The importance of addressing accountability of all roleplayers if a Pb(re)D approach is to be effective is further discussed in chapter 3. The term 'accountability', used in both GDPR and POPIA, is not defined in those statutes, but refers to taking responsibility for implementing data protection principles effectively.[220] As such, it is a corollary of the legal obligation to comply with data protection laws and the liability for failure to do so.

---

[215] POPIA s 1 '"Competent person" means any person who is legally competent to consent to any action or decision being taken in respect of any matter concerning a child;'

[216] POPIA s 35(1)(a) refers, in the singular, to the consent of 'a competent person'. This is a textual indication that the consent of a single parent should suffice. In the Children's Act 38 of 2005, s 18(4) provides that where more than one person has guardianship of a child, they may act independently, without consent of the others, save in relation to matters requiring consent by law, in ss (3)(*c*), whereas ss (5) requires that all guardians must provide consent.

[217] GDPR art 8(1).

[218] Ibid. As at 1 July 2019 the age of consent is 13 in Belgium, Denmark, Estonia, Finland, Latvia, Malta, Portugal, Sweden and the United Kingdom. The age of consent is 14 in Austria, Bulgaria, Cyprus, Italy, Lithuania and Spain. The age of consent is 15 in Czech Republic and France and has been included in draft legislation in Greece and Slovenia. See Ingrida Milkaite and Eva Lievens, 'The GDPR child's age of consent for data processing across the EU – one year later (July 2019)' (1 July 2019) <https://www.betterinternetforkids.eu/web/portal/practice/awareness/detail?articleId=3017751> accessed 22 August 2019.

[219] COPPA s 6501(1). The CCPA §1798.120(c) stipulates a requirement of express opt-in consent for the sale of personal information of any consumer who is less than 16 years of age. Consent must be given by a parent or legal guardian if the consumer is less than 13 years of age.

[220] Article 29 Data Protection Working Party, *Opinion 3/2010 on the Principle of Accountability* (WP 173, 13 July 2010) at 7.

XIII CONCLUSION

The introduction of POPIA will have an impact on a diverse range of laws and data practices. The focus of this study is on whether there is an 'accountability gap' in the selected legislation and a need for statutory reform to strengthen accountability for data protection under a Pb(re)D approach. The dissertation unpacks the concept of Pb(re)D and assesses its application and usefulness as a conceptual framework underpinning POPIA, in relation to the regulation of information processing by mobile apps. As the mobile apps ecosystem is a highly complex structure, involving terminology and practices that may be unclear to the layperson and lawyer alike, chapter 2 will provide the necessary context by defining key concepts referred to in this study, describing the role players in the mobile apps ecosystem and setting out important data-processing terms and practices.

TABLE 1 KEY DATA PROTECTION TERMINOLOGY

POPIA	GDPR	COPPA	CCPA
Personal Information[221]	*Personal Data*[222]	*Personal Information*[223]	*Personal Information*[224]
Information relating to an identifiable living natural person and, where it is applicable, an identifiable existing juristic person	Information relating to an identifiable living natural person	Information about an identifiable individual (but only where it is collected online from a child in the US)	Information about an individual (but only where they are a consumer in California)
		Expressly includes the parents of a child[225] and unique device identifiers.[226]	Expressly extends to the family and any device[227] of the individual

[221] POPIA s1.
[222] GDPR art 4(1).
[223] COPPA 15 USC §1605(8), expanded in COPPA Rule §312.2. It is common to see reference in US literature to 'personally identifiable information' (PII).
[224] CCPA §1798.140 (o)(1).
[225] COPPA Rule §312.2 (10).
[226] COPPA Rule §312.2 (7) defining 'persistent identifier' to include IP address, device serial number or unique device identifier.
[227] §1798.140 (p) defining 'probabilistic identifier' as permitting probable identification of a consumer or device.

Excludes deidentified information.[228] All personal information must be deleted. If it is reasonably possible to manipulate or link the information to other information to identify a data subject it remains personal information.	Excludes anonymised information[229] but includes pseudonymised information[230]	Excludes deleted information[231]	Excludes deidentified,[232] aggregated[233] and publicly available information. [234]
Responsible Party[235]	*Controller*[236]	*Operator*[237]	*Business*[238]
A person who alone or in conjunction with others determines the purpose and means of processing personal information	A person who alone or jointly with others determines the purpose and means of processing personal information	A person who operates a commercial website or online service directed at children, or with actual knowledge that they are collecting personal information from children.	A business in California that alone or jointly with others determines the purpose and means of processing personal information of consumers.

[228] POPIA s1, definition of 'de-identify', read with s6(1)(b).
[229] GDPR rec26. The term is not defined.
[230] GDPR rec 26 read with art 4(5), definition of 'pseudonymisation.' The information is no longer capable of identifying a data subject without the addition of other information held separately and subject to adequate safeguards against reidentification.
[231] COPPA Rule §312.2 defining 'delete'. Under COPPA if verified parental consent is not obtained to collect the personal information it must be deleted.
[232] CCPA §1798.140 (o)(3) read with §1798.140 (h), definition of 'deidentify'.
[233] CCPA §1798.140 (o)(3).
[234] CCPA §1798.140 (o)(2).
[235] POPIA s1.
[236] GDPR art 4(7).
[237] COPPA 15 USC §6501(2).
[238] CCPA §1798.140 (c). Although a business can take any form (including sole proprietors) it must be for profit Cand must have an annual turnover in excess of $25 million, or annually process the information of 50 000 consumers, households or devices, or receive more than 50% of its income from selling personal information.

Operator[239]	*Processor*[240]	---[241]	*Service Provider*[242]
Processing is outsourced to this person.			
Processing[243]	Processing[244]		
The actions[245] undertaken with personal information.		COPPA refers to the collection,[246] use,[247] maintenance,[248] disclosure[249] and release[250] of personal information	CCPA refers to the collection,[251] commercial use,[252] and sale[253] of personal information.
Data Subject[254]	*Data subject*[255]	*Child*[256]	*Consumer*[257]
This is the person to whom personal information relates. Under POPIA this includes natural and juristic persons.	This is the person to whom personal information relates.	A person under 13 and The parent of a child	A natural person resident in the state of California in their capacity as a consumer and The family,[258]

[239] POPIA s1. The operator acts under a contract or mandate with the responsible party without falling under their direct authority (i.e. not an employee).
[240] GDPR art 4(8).
[241] No specific term for the service provider is defined.
[242] CCPA §1798.140 (v).
[243] POPIA s1.
[244] GDPR art 4(2).
[245] POPIA s1 defines 'processing' as 'any operation, activity or set of operations concerning personal information'. GDPR, COPPA and CCPA refer in similar terms to the same activities.
[246] COPPA Rule CFR §312.2.
[247] Undefined.
[248] Undefined.
[249] COPPA 15 USC §6501(2).
[250] COPPA Rule CFR §312.2, which involves sharing personal information with third parties.
[251] CCPA §1798.140 (e).
[252] CCPA 1798.140 (f).
[253] CCPA §1798.140(t) (1).
[254] POPIA s1.
[255] GDPR art 4(1).
[256] COPPA 15 USC §6501(1) 'The term "child" means an individual under the age of 13.'
[257] CCPA §1798.140 (g).
[258] CCPA §1798.140 (x).

			household or device[259] of a consumer
---	*Third Party*[260]	*Third Party*[261]	*Third Party*[262]
	Defined negatively as anyone who is not the controller, or processor, i.e. someone who processes personal information for their own purposes.		

[259] CCPA §1798.140(j), e.g. a smartphone.
[260] GDPR art 4(10). COPPA and CCPA defines the term in a similar way. POPIA has no equivalent term. GDPR art 4(9) defines a 'recipient'as a person to whom personal information is disclosed, whether they are a third party or not. POPIA, COPPA and CCPA have no similar term.
[261] COPPA Rule §312.2.
[262] CCPA §1798.140 (w).

CHAPTER 2

THE MOBILE APPLICATIONS ECOSYSTEM

I INTRODUCTION

Mobile applications development is a new and rapidly growing field,[1] driven by the overwhelming popularity of smartphones for personal and business use.[2] As such, there is still much that has not yet been covered in reported legal decisions. The purpose of this chapter is to define key concepts,[3] describe the role players in the mobile applications ecosystem and set out important data processing terms and practices.[4] The chapter serves as a preface to the detailed analysis of data protection laws against a privacy-by-design framework. Two observations are important starting points.

First, the governance of the mobile apps ecosystem is complex as it involves multiple stakeholders: mobile app users, app developers, smartphone operating system (OS) developers, device (hardware) manufacturers, app markets, and a range of backend service providers (for example, providers of payment gateways), cloud platforms, and third parties

---

[1] Danial Johan Mohd Ridzuan Tan, Grace Yam Wen Tzi and Sian Lun Lau 'A study on cloud-based backend for crowd-sourced sensor datacollection apps' 2016 Institute of Electrical and Electronics Engineers (IEEE) Conference on e-Learning, e-Management and e-Services (IC3e) pages: 46–51 at 46.

[2]Mona Erfani Joorabchi, Ali Mesbah and Philippe Kruchten 'Real Challenges in Mobile App Development' 2013 ACM / IEEE International Symposium on Empirical Software Engineering and Measurement pages 15–24 at 15.

[3] The explanations and definitions are drawn from scholarly literature, industry publications and cross referenced to definitions in relevant statutes. This chapter is intended to provide a general understanding of key terms and does not purport to provide a technical explanation. For a glossary of terms relating to mobile in-app advertising see International Telecommunications Union Standardisation Sector (ITU-T), *Technical Framework for Countering Mobile In-Application Advertising Spam* (Recommendation ITU-T X1249, 2019). For a glossary of telecommunications terms see International Telecommunications Union (ITU), 'Telecommunication Terminology Database (TERMITE)' <https://www.itu.int/pub/S-TERM-DB> accessed 16 May 2020 and further standards on radio technology. For technical terms in software engineering generally see EEE Standards Board, *IEEE Standard Glossary of Software Engineering Terminology* (IEEE, New York, 1990) and IEEE, *P7012 - Standard for Machine Readable Personal Privacy Terms* (2017). For a glossary of fundamental concepts in digital technology see International Electrotechnical Commission (IEC), 'Digital Technology-Fundamental Concepts' <http://www.electropedia.org/iev/iev.nsf/index?openform&part=171> accessed 9 April 2020.

[4] This dissertation is concerned with data sharing between private corporations within the eco-system. Google and Apple publish transparency reports in which they detail information on inter alia legal subpoenas and government access requests through national security letters (NSLs) or under the Foreign Intelligence Surveillance Act of 1978, 50 U.S.C. §§ 1801 - 1885c (2018) (FISA) [Disclosure being limited in terms of the The Freedom of Information Act of 1966, 5 U.S.C. § 552 (2018) (FOIA, US).] Google Inc., 'Transparency Report' (2019) <https://transparencyreport.google.com/?hl=en> accessed 26 October 2019 and Apple Inc., 'Transparency Report' (2018) <https://www.apple.com/legal/transparency/> accessed 26 October 2019.

such as analytics companies, advertising networks and social networking sites.[5] It is not clear to what extent each of these parties is regulated by data protection laws. The problem is exacerbated because often these stakeholders will be based in multiple jurisdictions,[6] bringing into sharp focus the areas of conflict and ambiguity in legislation, and the weaknesses in cross-border co-ordination of enforcement.

Secondly, the data processing capabilities of mobile apps raise significant privacy concerns given the range of personal information that can be collected, but also because of the ubiquitous practice of sharing that data with third parties. Although there remains little quantifiable data about the mechanisms and extent of data sharing in the mobile ecosystem, it has been the subject of recent studies.[7] According to Wang, third party libraries[8] may account for as much as 60% of the code of mobile apps.[9] In a large survey of Google Play, 10 percent of apps sampled had at least one tracker, while seventeen percent had more than 20 trackers embedded in the app code.[10] Games and news apps had the highest percentage of trackers per app.[11] Approximately 10 percent of apps surveyed sent information to trackers in more than one jurisdiction.[12] Perhaps most concerning was the finding that there is a significant concentration of data flows. The root parent company of each tracker host was identified, and revealed that tech giants Alphabet (Google), Facebook, Twitter, Verizon, Microsoft and Amazon could control a large percentage of all data collected by mobile apps. Alphabet receives data from 88% of apps in the study.[13]

---

[5] Reuben Binns and others, 'Third Party Tracking in the Mobile Ecosystem' in *Proceedings of the 10th ACM Conference on Web Science* (ACM, Amsterdam, Netherlands 27–30 May 2018).
[6] Ibid. The study noted the most prevalent jurisdictions for third party trackers as the US, followed by China, Norway, Russia, Germany, Singapore, and the United Kingdom.
[7] See e.g. Yabing Liu, 'User Data Sharing in Online Services' (Northeastern University 2016) for a mechanism to quantify the value of user demographics in advertising via online social networks and identify the types of data third parties in the network have access to.
[8] Code written by third parties and embedded in mobile apps by the developer to enable a specific function, e.g. an advertisement (ad) library will enable the app to communicate with an ad server for in-app advertising.
[9] Haoyu Wang and Yao Guo, 'Understanding Third-Party Libraries in Mobile App Analysis' in *39th International Conference on Software Engineering Companion (ICSE-C)* (IEEE/ACM, Buenos Aires 20–28 May 2017).
[10] Binns and others. The study analysed 959 000 apps from the US and United Kingdom Google Play stores.
[11] Ibid.
[12] Ibid. This invokes the rules on cross-border transfers of data, which must be disclosed to app users.
[13] Ibid.

II DEFINITION OF KEY CONCEPTS

(a) The Mobile Application

The term mobile application (mobile app, or app) refers to a software application that runs on mobile wireless devices, such as smartphones, smartwatches and tablets.[14] The mobile app is capable of close interaction with the hardware and OS of the device through an application processing interface (API).[15] The term "mobile app" is used broadly in this dissertation to cover all apps regardless of installation mode, type or app category.

Apps can come pre-installed on the device or can be downloaded by the user from an app store or via a link on the app provider's website. There are three types of mobile apps.[16] Native apps run on the mobile device's OS, and the developer must be proficient in a compatible programming language[17] and write separate code for each OS platform. Web-apps run within a web browser on a mobile device. Hybrid apps are web-apps with a thin 'native wrapper' and can function across platforms.[18]

The rapid pace of innovative development has led to an app for virtually any conceivable facet of life. At the outset, apps were predominantly for utilities, such as the infamous Flashlight app.[19] Now there is a proliferation of apps of every type, and they are categorised in app stores by interest area such as gaming, news, entertainment, finance and education. Some apps are marketed aiming at individuals (consumers), whereas others are enterprise apps that may be installed by organisations on their employees' devices.

For the purposes of this study, the mobile app is treated as an object and not as a legal actor in its own right. Outlandish as the latter suggestion may initially sound, in terms

---

[14] International Telecommunications Union Standardisation Sector (ITU-T).
[15] Article 29 Data Protection Working Party, *Opinion 02/2013 on apps on smart devices* (WP 202, 27 February 2013) at 4.
[16] It is beyond the scope of this study to discuss the different technical considerations that may impact upon designing for privacy in each form of app.
[17] E.g. Java for Android and Objective C for IOS. See further Snigdha, '25 Best Programming Languages for Mobile Apps & Top Mobile App Development Tools & Frameworks' (18 Sept 2019) <https://www.appypie.com/app-development-guide> accessed 24 October 2019.
[18] Mona Erfani Joorabchi, Ali Mesbah and Philippe Kruchten, 'Real challenges in mobile app development' in *Proceedings of ACM/IEEE International Symposium on Empirical Software Engineering and Measurement* (ACM/IEEE, Baltimore, Maryland 10–11 October 2013); Ming Xu, 'A System Perspective to Privacy, Security and Resilience in Mobile Applications' (University of Saskatchewan 2019) at 8.
[19] The developers of the 'Brightest Flashlight' app faced regulatory action in the US. See *In the matter of Goldenshores Technologies, LLC and Erik M. Geidl* FTC Dkt No C-4446 (Apr 9, 2014) (consent order) discussed in chapter 2 and 4.

of the Electronic Communications and Transactions Act 25 of 2002 (ECTA), a mobile app is an 'electronic agent',[20] capable of initiating the collection and further processing of personal information without direct human intervention (that is, it acts as an 'automated transaction').[21] Nevertheless, in terms of section 20 of ECTA, any party using the electronic agent is bound by any agreement reached.[22] The legal accountability of those parties, and not the legal role of the mobile app itself, is what is central to this study.

(b) The User Interface (UI) and User Experience (UX)

The User Interface (UI) refers to the screen visible to the user when he or she is running the application. Some of the development constraints presented by mobile devices is their small screen size and touch screen operation, as well as limited storage, computational capacity and battery power.[23] Thus the design of the UI[24] is key to designing for a satisfying mobile application user experience (UX).[25] The narrative of 'design' in the mobile app ecosystem is thus centred in this paradigm, which is not to be confused with the concept of 'privacy by design'.[26]

(c) The Application Processing Interface (API)

An application processing interface (API) is a set of programming instructions and standards that permits communication between applications.[27] Through the OS API, app developers are able to read and write data such as contents and calendar entries, record audio, use the camera,

---

[20] The Electronic Communications and Transactions Act 25 of 2002 (ECTA) defines 'electronic agent' as 'a computer program or an electronic or other automated means used independently to initiate an action or respond to data messages or performances in whole or in part, in an automated transaction'.

[21] In terms of ECTA s 1: '"automated transaction" means an electronic transaction conducted or performed, in whole or in part, by means of data messages in which the conduct or data messages of one or both parties are not reviewed by a natural person in the ordinary course of such natural person's business or employment.'

[22] E.g. an e-commerce app where purchases are concluded through the mobile app without review by a natural person for the seller.

[23] Xu at 8.

[24] Design considerations are constrained by the device itself, and involve making optimal use of appropriately sized buttons, icons, input areas, menus and filters.

[25] Xu at 20.

[26] Heather Burns, 'How To Protect Your Users With The Privacy By Design Framework' (27 July 2017) <https://www.smashingmagazine.com/2017/07/privacy-by-design-framework/> accessed 26 October 2019.

[27] Dave McComb, *Semantics in business systems: The savvy manager's guide* (Morgan Kaufmann 2004) at 334 defines an API as '[a] published interface to an application or module that allows the programs to call or invoke services.' In software engineering a 'call' is '[a] computer instruction that transfers control [over data or a function] from one software module to another'. Institute of Electrical and Electronics Engineers (IEEE) Standards Board at 14.

access photographs, read, modify and delete information stored on the SD card,[28] read the phone state to know when it is on charge, 'wake up' the device or prevent it from 'sleeping', collect unique device identifiers and modify system settings such as Wi-Fi on/off.[29]

(d) Third Party Library

The term 'third party library' refers to code (a 'software development library'[30]) that has been written by a third party and which the app developer has embedded in ('copied into') the app code. The library communicates with the app via the library's API. As such, a 'third party library' might be referring to code of a backend service provider, or some other operator (processor), or it could be referring to a true third party, as the term is used in this dissertation.

Given the constraints placed upon app developers by clients and market competition, reliance on third party libraries is ubiquitous, as it would be unnecessarily time consuming and costly for app developers to write all code from scratch. Users benefit when the third party library permits improved functionality within the app. Such code can be licensed, proprietary or open source. The use of open-source APIs is particularly crucial to the software development industry as it lowers the cost and time of development for small, independent developers.[31] The term does not refer to malicious code that enables unauthorised parties to gain access to information. However, when app developers make injudicious use of untested third party code, they could unwittingly introduce malicious or insecure code into the app. [32]

---

[28] An SD-card is the 'secure digital' memory card in a smart device, and is named after the developer of the standard, the SD Association (SDA).

[29] Article 29 Data Protection Working Party.

[30] Institute of Electrical and Electronics Engineers (IEEE) Standards Board at 67 defines the term as '[a] software library containing computer readable and human readable information relevant to a software development effort'.

[31] Amicus curiae submissions of Developers Alliance in *Oracle America Inc. v Google Inc.* 886 F3d 1179 (Fed Cir 2018). The decision held that Oracle America's Java script API was copyrightable and held that Google's use of Java in early versions of its Android OS fell outside 'fair use'. The decision reversed earlier District Court judgments, and the case will be heard on appeal before the US Supreme Court on 7 October 2020. (Case information appears on the website of the US Supreme Court, <https://www.supremecourt.gov/search.aspx?filename=/docket/docketfiles/html/public/18-956.html> accessed 22 July 2020.

[32] For the latest scholarship on mitigating privacy risks introduced by third party libraries in m-health, ride-hailing and activity-tracker apps see Thi Van Anh Pham, *Privacy-Enhancing Technologies for Mobile Applications and Services* (2019).

(e) Software Development Kit (SDK)

A software development kit (SDK) is 'a set of software development tools that allow for the creation of applications for a certain software package, software framework, hardware platform, computer system, video game console, operating system, or similar development platform'.[33] An SDK is thus similar to an API, but contains a complete range of programming tools and supporting documents. A developer will typically not write custom code for the whole application, but will use one or more APIs, third party libraries and SDKs.

(f) The Operating System

A mobile operating system (mobile OS) is a software platform on top of which application programs can run on a mobile device.[34] Google's Android OS and Apple's IOS are dominant in the mobile environment, with a 76.24% and 22.48% market share respectively.[35] While Android was developed as an open-source software platform and can function on a range of devices, IOS is proprietary to Apple. Some devices run on a licensed operating system.[36]

(g) Permissions

A permission governs when an OS will allow a mobile app to access data or resources on the device.[37] An app developer must define these 'permission requests' in the app manifest that must accompany the submission of the app for publication in the app store. Correct use of permission requests is a key factor in app store review guidelines.[38] Broadly, one can distinguish between 'dangerous' permissions, which require the permission request to be

---

[33] Xu at 11.
[34] OO Okediran and others, 'Mobile Operating Systems and Application Development Platforms: A Survey' (2014) 6 *International Journal of Advanced Networking and Applications* 2195–2201.
[35] Statcounter, 'Mobile Operating System Market Share Worldwide' <https://gs.statcounter.com/os-market-share/mobile/worldwide> accessed 24 October 2019. For a full discussion of these two development environments (Android and IOS) see Xu.
[36] Fling at 20.
[37] For an overview of permission in the Android and iOS environment see Google Play Developer Policy Centre, 'Permissions' <https://play.google.com/about/privacy-security-deception/permissions/> accessed 31 August 2019 and Apple Developer Centre, 'Requesting Permission' <https://developer.apple.com/design/human-interface-guidelines/ios/app-architecture/requesting-permission/> accessed 31 August 2019.
[3838] For the review guidelines of the Google Play Store and Apple App Store see Android Developers, 'Launch checklist' (27 December 2019) <https://developer.android.com/distribute/best-practices/launch/launch-checklist> accessed 9 April 2020 and Apple, 'App Store Guidelines' (12 September 2019) <https://developer.apple.com/app-store/review/guidelines/> accessed 28 February 2020. Creating a developer account with Google and Apple requires agreement to abide by all applicable policy documents. These terms are discussed later where relevant.

specifically granted by the user and relate to 'sensitive' information; and normal permissions, which may be granted automatically. However, as each OS defines permissions in accordance with its own security architecture, there are differences in how privacy is protected.

Google was criticised for grouping all permission requests at installation, and not giving users an option to revoke permissions.[39] Apps running on Android 6.0 (Marshmallow) (released on 5 October 2015) and SDK version 26, or higher, must now request dangerous permissions[40] at runtime (that is, when the permission is first needed while the app is in use), and additional user controls allow permissions to be delayed, revoked or varied.[41] While user control has been enhanced, users may not be aware that permissions are organised in groups and that if they grant a permission request in a particular group, the app will automatically grant all future permission requests in the same group without user notification.[42] For example, if an app requests permission to read contacts, the user will be prompted to give permission to 'access contacts', so that if the app later requests to 'write contacts' the permission will be automatically granted.[43]

Normal permissions allow the application to access information that poses very little risk to user privacy or the operation of other apps. [44] Such permissions are granted automatically on installation without notification to the user.[45] Signature permissions are granted on installation where the app is signed by the same certificate as another app that defines the permission.[46] For users, this means that if permission has been granted in one app, it may not be asked for again in another app – and there does not appear to be any notification to the user that this has occurred, or that permissions can be revoked on an app-by-app basis, in this case.

---

[39] Ilias Leontiadis and others, 'Don't Kill My Ads!: Balancing Privacy in an Ad-Supported Mobile Application Market' in *Proceedings of the Twelfth Workshop on Mobile Computing Systems & Applications* (ACM February 2012).
[40] There is no longer a table of dangerous permissions and permission groups included in the Android Developers' 'Permissions Overview' <https://developer.android.com/guide/topics/permissions/overview#dangerous_permissions> accessed 31 August 2019.
[41] Ibid. Also see Google Play Developer Policy Centre.
[42] Android Developers, 'Permissions Overview'.
[43] Ibid.
[44] Ibid.
[45] Ibid.
[46] Ibid.

(h) Broadcasts

Apps send and receive data about events using broadcasts. Apps can send custom broadcasts to other apps, for example, when a user downloads new content.[47] Apps can also register in the app manifest to receive broadcasts from the OS about 'system events', such as when the user boots up or places the device on charge.[48] Explicit broadcasts are sent only to a specific app. Implicit broadcasts will be sent to all apps that have registered to receive them. Following the introduction of Android Oreo (8.0) on 21 August 2017, apps targeting Android 8.0 are no longer permitted to receive most implicit broadcasts.[49]

(i) Background Processing

To avoid slowing down app performance (which would impair the user experience), apps are configured to run most processes on a background thread, meaning that the main thread which controls the user interface co-ordinates only processes that involve user interactions.[50]

Thus, even if a user is not interacting with an app, or even when the app is not open in the foreground, it may continue running in the background.

Apps can also register to receive background location updates. Many users may assume that when an app requests permission to access location, that the app will only do so when the user is interacting with the app. In fact, once the permission has been granted the app could receive continuous real-time updates of the user's location based on the smartphone's GPS coordinates for as long as it remains installed on the device. In Android 10 (released on 3 September 2019), a new permission to 'ACCESS_BACKGROUND_LOCATION' has been introduced.[51] However, unless the user has refused permission to access any location, permission to access background location will continue to be automatically granted on apps targeting Android 9 or lower, and apps targeting

[47] Android Developers, 'Broadcasts Overview' <https://developer.android.com/guide/components/broadcasts> accessed 19 February 2020.
[48] Ibid.
[49] Android Developers, 'Implicit Broadcast Exceptions' <https://developer.android.com/guide/components/broadcast-exceptions.html> accessed 19 February 2020.
[50] Android Developers, 'Guide to Background Processing' (27 December 2019) <https://developer.android.com/guide/background> accessed 19 February 2020.
[51] Android Developers, 'Privacy changes in Android 10' (27 December 2019) <https://developer.android.com/about/versions/10/privacy/changes> accessed 19 February 2020.

Android 10 installed on devices running an earlier version of Android (even if they later upgrade to Android 10).[52]

For developers, this is primarily a user experience concern because it drains the battery and slows overall phone performance,[53] but it raises data protection concerns about the transparency of such practices. In Android Oreo 8.0+ automatic limits have been placed on background execution, and users can enable these settings in earlier versions.[54] Android Oreo has also introduced background location limits, but these limits still permit apps to request location updates a few times an hour.[55]

(j) The Device (Hardware)

The terms 'device', 'hardware' or 'terminal equipment' refer in this context to the smartphone, tablet or wearable article on which the mobile application is installed. The device, and any information stored on it, must be regarded as part of an individual's 'private sphere'[56] and the availability of means to access that information secretly, or trace a user's activities without their knowledge, may constitute a serious invasion of privacy.[57]

With nearly one hundred device manufacturers, there is a proliferation of mobile phone brands, each with its own unique form factor[58] and hardware configuration,[59] but a common constraint is the small screen size of mobile devices which makes it more difficult to communicate privacy notices to users.[60] The device (hardware) communicates with each application (software) loaded on the phone through an API. Although industry

---

[52] Ibid.
[53] Android Developers, 'Background Execution Limits' (27 December 2019) <https://developer.android.com/about/versions/oreo/background#broadcasts> accessed 19 February 2020.
[54] Ibid.
[55] Android Developers, 'Background Location Limits' <https://developer.android.com/about/versions/oreo/background-location-limits.html> accessed 19 February 2020.
[56] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector 2002/58/EC (e-Privacy Directive) OJ L 201/37, 31.7.2002, rec 24.
[57] Ibid.
[58] Form factor refers to the size, shape, and style of the phone (e.g. flip phone, touchscreen, and tablet) and the layout and position of its components. Wikipedia, 'Form Factor (Mobile Phones)' <https://en.wikipedia.org/wiki/Form_factor_(mobile_phones)> accessed 19 February 2020.
[59] GSM Arena, 'All Mobile Phone Brands' <https://www.gsmarena.com/makers.php3> accessed 24 Ocobert 2019.
[60] Paula J Bruening and Mary J Culnan, 'Through a Glass Darkly: From Privacy Notices to Effective Transparency' (2016) 17 *NCJL & Tech* 515–580 at 564.

standards have been developed, device manufacturers can interpret those standards differently, resulting in differences in how content is displayed across devices.[61] This can affect the user experience of an app, but also has implications for how permission requests are displayed, and the settings to revoke or amend permissions. The design of the device can have a long-lasting impact on privacy.[62] Even if an update of the OS version or mobile app version improves privacy settings, a user cannot benefit if the device does not support that functionality. Likewise, not all devices support automatic encryption of data stored on the device, access controls such as biometrics or PIN or password and multi-factor authentication protocols. [63] Lastly, co-operation is required from device manufacturers, OS platforms and carriers to detect security vulnerabilities and test updates. Despite industry efforts, the proliferation of device types means that there are still significant delays between the discovery of vulnerabilities and the release of security patches.[64]

(k) The Mobile Applications Ecosystem

In this dissertation, the term 'mobile applications ecosystem' is used to describe the parties involved in the creation and deployment of mobile apps.[65] Privacy by design cannot be

---

[61] Fling at 20.

[62] A Cavoukian and M Prosch, *The Roadmap for Privacy by Design in Mobile Communications: A Practical Tool For Developers, Service Providers, and Users* (Toronto, ON, Canada: Office of the Privacy Commissioner, Ontario, Canada, 2010) at 11.

[63] Ibid at 11, where Cavoukian and Prosch note that an expert industry panel convened for the Arizona State University (ASU) Privacy by Design Lab's study on mobile technologies recommended that all devices should support 'automatic, seamless encryption of data stored on the device', multi-factor authentication and enforced PIN/password lock protection. Newer Android devices now support encryption, and it has been made a default 'out the box' setting in Android Nougat. Adoption rates were considerably lower with Android Marshmallow where encryption had to be enabled by the user, and lower still on earlier versions where encryption negatively impacted device performance. See figures provided by Google in 2017 and quoted by Oleg Afonin, 'Android Encryption Demystified' (23 May 2017) <https://blog.elcomsoft.com/2017/05/android-encryption-demystified/> accessed 19 February 2020. The data stored on an Apple smartphone is encrypted by default when the device has a passcode or Touch ID enabled during device set up. ICloud back-up is also encrypted by default but in iTunes encryption must be enabled by the user. Kaspersky, 'iPhone Encryption: How to Encrypt Your iPhone' <https://usa.kaspersky.com/resource-center/preemptive-safety/iphone-encryption> accessed 19 February 2020.

[64] Federal Trade Commission, *Mobile Security Updates: Understanding the Issues* (February 2018) at 65. The availability of device update support and update frequency remains highly variable within the industry.

[65] Federal Trade Commission, *Beyond Voice: Mapping the Mobile Marketplace* (April 2009). The report illustrates the early struggle to develop application utility that today's consumers take for granted. E.g. If applications could not share data it would not be possible to find a restaurant in mobile browser, open directions in a mapping app, dial the restaurant and save the phone number in contacts for future use. The report using the term 'mobile ecosystem' to differentiate this nascent market from the desktop environment. In 2020, however, the emphasis is on a 'seamless' or 'frictionless' user experience across devices so that the boundaries between desktop and mobile are increasingly becoming blurred. User data could be collected from a browser to direct a user to the same content inside an app (via a link to the app installed on the user's device or via a link to download

achieved without the involvement of all role-players in the mobile apps ecosystem.[66] While some role-players will bear primary responsibility for certain issues, responsibility cannot be assigned exclusively to any single role-player.[67] Further, as mobile apps are built on device hardware, software and APIs that have already been designed, there is a need to re-think how privacy by (re)design can best be addressed.[68]

III PRINCIPAL PARTIES IN THE MOBILE APPLICATIONS ECOSYSTEM

There are three principal parties in the mobile apps ecosystem: the app user, the app developer and the app owner.

(a) The User

The user refers to the individual who is using the application on a mobile device. The user may be an adult who is the owner of the device, a subscriber to a cellular service connected to the device, and the holder of an Apple or Google account associated with the device. However, the user of the device may also be another member of the device owner's household, including a child. In all instances, insofar as the application processes the user's personal information, that person will be the 'data subject' referred to in data protection legislation. However, users may also interact with the application to post content about themselves or other individuals, which may in certain circumstances make them a responsible party in

---

the app sent by SMS or email, or shared from a 'friend' on a social networking site which will take the user the same content after installation (and log the data for app installation and user engagement statistics).

[66] Cavoukian and Prosch at 7.

[67] Ibid. The importance of this point merits quoting in full from the report: '"Privacy by Design is a team sport". No single designer can achieve privacy within an organization, and no single organization can achieve privacy within an industry. Concurrent with traditional, internal considerations such as the Privacy Impact Assessment, privacy/security Gap Analysis, and the Threat Risk Assessment, each of which is becoming common practice within numerous industries, privacy must be considered in a holistic, ecosystem-wide manner if it is to be both effective and lasting. It is notable, then, that while the expert panel in some cases heavily weighted responsibility for a solution towards a single party, there was no solution for which all of the expert panellists agreed that responsibility could be assigned exclusively to a single party.'

[68] See generally A Cavoukian and Claudiu Popa, *Privacy by ReDesign: A Practical Framework for Implementation* (Toronto, ON, Canada: Office of the Privacy Commissioner, Ontario, Canada, 2011), and the detailed discussion in chapter 3.

relation to their processing of such personal information,[69] save for purely personal or household use.[70]

(b) The App Developer

The term 'app developer' is a broad term for a widely diverse set of persons that develop (or 'build') mobile applications.[71] There is no official statistic for the numbers of app developers worldwide, but a 2016 industry report placed the figure at 8.7 million mobile app developers at that time.[72] Such app developers are typically young and overwhelmingly male. Geographically, app developers are concentrated in Asia, Europe and the US, with only 70 000 (3%) based in Africa.[73] While some are professional developers,[74] the majority develop apps as a 'hobby' or 'side project',[75] and thus formal educational qualifications and industry training are also highly variable amongst app developers.[76]

---

[69] Article 29 Data Protection Working Party, *Opinion 5/2009 on Online Social Networking* (WP 163, 12 June 2009) at 6.

[70] Processing for purely household use is excluded under POPIA s 6(1)(a) and GDPR art 2(2)(c). A full discussion of the scope of this exclusion, and the responsibility of users for the processing of personal information is beyond the scope of this dissertation. However, it should be made clear that a responsible party must be processing his or her own household activities to qualify for the exemption. This is made explicit in GDPR as art 2(2)(c) is restricted to processing by natural persons, with no professional or commercial connection. It does *not* exempt the providers of services used in the household, and a fortiori where a mobile app developer is collecting personal information on a data subject's household activities that information is part of the private sphere. Nomalanga Mashinini 'The processing of personal information using remotely piloted aircraft systems in South Africa' (2020) 53 (1) *De Jure* 140–158 at 151 asserts that there is a 'gap' in POPIA where aerial drones are used to 'look' in to private homes, as purely household information is 'excluded' from POPIA. This is a misinterpretation of the Act that is inconsistent with the clear imperative in s 2(a) read with s 3(3)(a) of the Act that it must be interpreted in a way that upholds the right to privacy.

[71] European Union Agency For Network and Information Security (ENISA), *Privacy and Data Protection in Mobile Applications: A Study on the App Development Ecosystem and the Technical Implementation of GDPR* (November 2017).

[72] Artyom Dogtiev, 'Mobile App Developer Statistics Roundup' 'https://www.businessofapps.com/news/mobile-app-developer-statistics-roundup/' (20 January 2016) <https://www.businessofapps.com/news/mobile-app-developer-statistics-roundup/> accessed 28 February 2020, cited in Federal Trade Commission, *Mobile Security Updates: Understanding the Issues* at 18.

[73] Dogtiev. In Africa 91% are male, and the average age is 27.

[74] A professional developer may be employed either for a large corporate developing in-house apps (e.g. financial services companies and large retailers) or by small or medium-sized IT company offering mobile app development services.

[75] Dogtiev.

[76] Cf the situation where an online survey conducted by the Developers Alliance in 2012 in the US found most developers were professionals with a college degree in their mid-thirties. Nevertheless it is noteworthy that two-thirds were still employed by small firms (defined in the survey as 3 employees or less). The survey received 352 respondents. See Rachel Emeis, 'Preliminary Report from the 10-City Application Developers Alliance Privacy Summit Series' (29 November 2012) <https://www.developersalliance.org/press-releases/preliminary-report-from-the-10-city-application-developers-alliance-privacy-summit-series> accessed 2 March 2020. As the survey distribution coincided with the Developer's Alliance Privacy Summit (which took place across 10 US cities during 2012), there may be an element of response bias which resulted in oversampling professional

These app developers will typically not write all the app code themselves, making wide use of third party SDKs and libraries that are integrated into the app. There are many reasons for this. Some developers lack the technical skill to write the code themselves, but using third party code also substantially reduces the cost and time of development in a competitive market, can enhance functionality and user experience, and is used to monetise the app through advertising or in-app purchases.[77] Similarly, once the app is deployed (even when the app developer is also the app owner), the actual processing of personal information will often take place in the mobile cloud, making it very important to analyse carefully the legal accountability of all parties.

(c) The App Owner

The app owner (or app publisher) is the entity that offers the app to end-users.[78] When a native app is distributed on the Apple App Store or the Google Play store, the developer is listed in the app information. This company is considered the app developer 'regardless of whether it wrote the app's code itself, integrated code from mobile SDK developers and/or obtained the services of a software developer vendor who actually wrote the code for the app'.

However, from a legal perspective, it is important to distinguish between app developers who distribute their own apps on an app marketplace (in which case they are also the app owner) and those that develop apps for clients. In the latter instances, the client would be the app owner (or app publisher).[79]

This raises important issues about the responsibility of each party for ensuring that data protection principles are implemented in the design and throughout the development

---

developers. Also see Mark Mulligan and David Card, *Sizing the EU App Economy* (Gigaom Research and European Commission Eurapp Project, February 2014) at 11–12. Most developers, scripters and coders had a college degree, but the majority were employed as small independent developers with less than 3 years' experience.

[77] A 'free' or 'freemium' app can be downloaded from the app store at no cost but will typically be monetised through in-app advertising. As the developer is paid by an advertiser on an advertising network, based on the number of clicks on the advert in the app, the ad library must be incorporated into the code of the app. Developers also rely on in-app purchases (e.g. to level up in games, or buy premium content), or app subscriptions (after a free trial period), which are facilitated by payments through the app store (iTunes or Google Play account) via code in the Android or iOS developers' SDK. E-commerce apps may enable a payment gateway, such as PayPal, which requires incorporate of the service provider's code into the app. In addition, apps may monetise user data by selling aggregated or anonymised data, such as market reports, or selling personally identifiable information to data brokers.

[78] ENISA at 9.

[79] Ibid at 9.

and testing of the app, but also after the deployment of the app.[80] For developers who continue to 'host' the app after its market release, questions arise about 'ownership' of the data collected by the app. Those issues are impacted not only by data protection legislation but also by the terms and conditions upon which the app developer was contracted by the app owner.[81]

IV GATEKEEPERS IN THE APP ECOSYSTEM

I use the term "gatekeepers" to refer to the parties that stand between the user and the developer, and through the design of their own product or service have the means of constraining the privacy risks posed by mobile apps. These parties are the app marketplaces, the owners of the operating systems, mobile network operators, internet service providers, device manufacturers and online social networking platform providers.

(a) The App Marketplace

App marketplaces are distribution platforms where apps can be listed by developers (publishers) for download by users. The two largest app marketplaces are the Apple App Store and the Google Play store. Thus, in the Apple development environment, Apple is the device manufacturer, and the owner of the OS and app store relevant to those devices. In the Android development environment, a wide range of devices can run Android, but Google is the owner of the OS and the app store, as well as a range of analytics and advertising subsidiaries.

In addition to Apple and Google, there are numerous smaller native app distribution platforms: Amazon, Microsoft, Blackberry, Samsung Galaxy and Ubuntu, and a host of alternative app marketplaces: Appland, Aptoid, Café Bazaar, Cydia, F-Droid, GetJar, Mikandi and Opera.[82]

The terms upon which an app is listed, or removed, from the App Store, are contained in the app store's developer contract, policies and terms of use. App store review

[80] Ibid.
[81] Consideration of the relationship between app developer and app owner, and the terms upon which they contract, as well as the important questions around who owns the data, is beyond the scope of this dissertation.
[82] 'List of mobile app distribution platforms' (20 September 2019) <https://en.wikipedia.org/wiki/List_of_mobile_app_distribution_platforms> accessed 24 October 2019.

guidelines and the review process have become more comprehensive, in response to the existence of malicious applications in app stores.[83]

he case of Google, the primary contract is the Google Play Developer Distribution Agreement,[84] which incorporates by reference (in section 4.1) all the policies in the Developer Policy Centre,[85] and also binds developers, in section 9.1, to uphold the Google Privacy Policy.[86] An app developer wishing to distribute an approved app for download from the Google Play store will be issued with a unique signing key to secure the .APK file[87] that users will install. This key can be stored by Google Play, in which case the developer must agree to the Google Play App Signing Terms of Service as well. Google's relationship with a user of any Google product or service is governed by the privacy policy and by Google's Terms of Use.[88] In essence the policy framework makes the app developer soley responsible for data privacy in the app,[89] but records that Google will receive information (some of which is also available in the form of aggregated statistics to the developer) 'order to continually innovate and improve Google Play, related products and services, and the user and Developer

[83] Lorin Wu, 'Apps Disguised as Security Tools Bombard Users With Ads and Track Users' Location' (3 January 2018) <https://blog.trendmicro.com/trendlabs-security-intelligence/apps-disguised-security-tools-bombard-users-ads-track-users-location/> accessed 28 February 2020. The study discovered 36 apps labelled as security tools, but which were actually malware designed to push ads and collect personal information (which included Android ID, MAC address, IMSI, OS, location, installed apps and contents of the notification bar). The 'security notices' were fake designed to legitimise the app and increase click through rate on ads displayed. Google Play removed the apps.

[84] Google, 'Google Play Developer Distribution Agreement' (15 April 2019) <https://play.google.com/about/developer-distribution-agreement.html> accessed 24 October 2019. After this dissertation was submitted for examination Google published a substantial revision of the agreement effective from 17 November 2020. The amendments are prima facie aimed at complying with GDPR, and this may signal a positive shift but an empirical analysis of whether the suite of Google contracts and policies align with PbD principles lies beyond the scope of this dissertation.

[85] Google, 'Google Play Developer Policy Centre' <https://play.google.com/intl/en-US/about/developer-content-policy-print/> accessed 24 Oct 2019. The developer must also comply with Google's brand guidelines

[86] Google LLC., 'Google Privacy Policy' (15 October 2019) <https://www.gstatic.com/policies/privacy/pdf/20191015/9ad23b47/google_privacy_policy_en.pdf> accessed 24 October 2019.

[87] APK stands for Android Package Kit – the package file format used by the Android operating system for distribution and installation of mobile apps.

[88] Google LLC., 'Google Terms of Service' (25 Oct 2017) <https://policies.google.com/terms?hl=en&gl=us> accessed 24 October 2019.

[89] Clause 11.3 of the Google Play Developer Distribution Agreement states: 'You represent and warrant that, as the principal to the transaction with the user, You are solely responsible for compliance worldwide with all applicable laws and other obligations.' This remains unchanged in the updated 17 November 2020 version.

experience across Google products and services.'[90] In the case of Apple, the primary contracts are the Apple Developer Agreement,[91] app review guidelines[92] and Apple Privacy Policy.[93]

(b) The Owner of the Operating System

It is the operating system (OS) that controls what device data and resources are made available to an application, and the structure and timing of permission requests. While there is an obligation on application developers not to request access to data and resources that the app does not need, it is the OS that determines whether it is possible to request such access, whether the app developer can tailor access to only such data as is needed,[94] and whether and how the user will be notified. Thus the owner of the OS is a 'key enabler' of privacy in the mobile ecosystem.[95] Likewise, the 'fine-grained' privacy controls are instantiated at the OS level.[96] In other words, it is the OS that determines how easy it is for users to set privacy preferences[97] and use privacy features built into the device. The most recent studies show that leaks of private data and circumvention of permission settings remain problematic.[98]

---

[90] Clause 9.2 of the Google Play Developer Distribution Agreement. Significantly, however, from 17 November 2020, this collection is further regulated by the 'Google Controller-Controller Data Protection Terms' < https://privacy.google.com/businesses/gdprcontrollerterms/> accessed 8 February 2021, which incorporates the Standard Contractual Clauses on transfers from the EU to a non-EU controller. Impliedly Google recognises that insofar as it receives data it is a 'controller'. See Google, 'Google Controller-Controller Data Protection Terms: Standard Contractual Clauses; SET II - Standard contractual clauses for the transfer of personal data from the Community to third countries (controller to controller transfers)'
'<https://privacy.google.com/businesses/gdprcontrollerterms/sccs/> accessed on 8 February 2021. Analysis of these developer contracts lies outside the scope of this dissertation.

[91] Apple Inc., 'Apple Developer Agreement' <https://developer.apple.com/terms/apple-developer-agreement/Apple-Developer-Agreement-English.pdf> accessed 24 Oct 2019. Developers must also agree to the terms of use governing Apple's intellectual property, developer forums, the Apple website and the licensing agreement (of Apple's proprietary software) appropriate for the type of developer account.

[92] Apple Inc.

[93] Apple Inc., 'Apple Privacy Policy' (29 August 2019) <https://www.apple.com/legal/privacy/en-ww/> accessed 26 October 2019.

[94] Cavoukian and Prosch at 16 refer to the example of access to location services. See the discussion of location services below.

[95] Ibid at 14.

[96] Ibid.

[97] Ibid at 14–15. The report evaluates OS settings by three user-centric criteria: accessible from the home screen, understandable (through clear explanations) and comprehensive, providing cross-app controls where possible, and providing a seamless user privacy experience by making it possible for app developers to incorporate privacy functions into an app through the API.

[98] Benjamin Eric Andow, 'Privacy Risks of Sensitive User Data Exposure in Mobile Ecosystems' (DPhil (Computer Science), North Carolina State University 2019); Jianmeng Huang and others, 'SieveDroid: Intercepting Undesirable Private-Data Transmissions in Android Applications' (2019) 14 *IEEE Systems Journal* 375–386; Abraham H Mhaidli, Yixin Zou and Florian Schaub, '"We Can't Live Without Them!" App Developers' Adoption of Ad Networks and Their Considerations of Consumer Risks' in *Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)* (USENIX, Santa Clara, CA, USA 11–13 August 2019) Joel

(c) Electronic Communications Service Provider (ECSP)

The term 'electronic communication service provider' (ECSP) is a broad term that refers to the provider of any electronic communication service.[99] This includes a mobile network operator (MNO) and an internet service provider (ISP), and both play a key role in the mobile apps ecosystem, as described below.

(d) Mobile Network Operator (MNO)

A mobile network operator (MNO), also known as a cellular service provider or carrier, operates the cellular network[100] (and may control related infrastructure and radio frequency spectrum allocation) that makes telephony and internet access using cellular data available to their subscribers (smartphone users), whom they bill for the services. The speed and capability of the network and the cost of data impact upon the performance of mobile applications. Operators often sell mobile devices (handsets) to their subscribers (at discounted prices) with preloaded content and services to lock subscribers into contract deals,[101] and to capture data for monitoring network and device faults.[102] The MNO also has access to the data that is transferred over their network and to communications between the smartphone and the cell towers on the network.

(e) Internet Service Provider (ISP)

The term 'Internet Service Provider' (ISP) is a broad term for any party that provides its clients with access to the internet. Access ISPs provide access to wired (DSL, cable and fibre) internet

---

Reardon and others, '50 Ways to Leak Your Data: An Exploration of Apps' Circumvention of the Android Permissions System' in *Proceedings of the 28th USENIX Security Symposium* (USENIX, Santa Clara, CA, USA 14–16 August 2019); Jingjing Ren, 'Measuring Personal Information Exposure in the Mobile and IoT Environments' (Northeastern University 2019) and Trishita Tiwari and others, 'Location Leakage from Network Access Patterns' in *2019 IEEE Conference on Communications and Network Security (CNS)* (IEEE, Washington DC 10–12 June 2019).

[99] The Electronic Communications Act 36 of 2005 defines an 'electronic communications' as including 'voice, sound, data, text, video, animation, visual images, moving images and pictures, signals or a combination thereof' but excluding 'content services'.

[100] Federal Trade Commission, *Mobile Security Updates: Understanding the Issues* (attachment A) defines carrier as the 'operator of a cellular network'.

[101] Ibid. A 'carrier-locked device' means 'a smartphone, tablet, or similar mobile computing device that can connect to a particular carrier's cellular network and is restricted via software to work only on that carrier's network.' A 'carrier-certified device' means 'a smartphone, tablet, or similar mobile computing device that is not a carrier-locked device but has been certified by a carrier to be sold through that carrier or activated on that carrier's network.' Also see Fling at 19.

[102] See for example the use of Carrier IQ software by Sprint and AT&T in the US, *In re Carrier IQ, Inc. Consumer Privacy Litigation* Case No 12-md-02330 EMC (NC) (ND Cal Sep 27, 2013).

via a local area network (LAN) and broadband wireless internet (Wi-Fi). Wi-Fi-enabled smart devices can thus connect to the internet. Smartphone owners can contract with an ISP if they are using Wi-Fi on a home network.[103] In such cases, the manufacturer of the router also bears responsibility for the security of the home network and any cloud storage offered by the router for data syncing across devices.[104]

ISPs can also provide hosting services for email, websites and data storage, and may thus be contacted as a back-end service provider to the app developer or app owner. ISPs have access to the data that is transferred via their networks.[105] An ISP is an 'electronic communications service provider',[106] although not all its services will be electronic communications services.[107]

(f) Device Manufacturers

A device manufacturer is the 'entity that designs or develops [a smartphone, or other mobile device] that is offered for sale to consumers'.[108] The term is used here to include an original equipment manufacturer (OEM)[109] and a chipset manufacturer.[110] Device manufacturers play an important role in how content is displayed and how applications function on devices (as discussed above). Additionally, device manufacturers may distribute devices with certain features, such as GPS location tracking, enabled by default,[111] and with a range of pre-

---

[103] When using free Wi-Fi in public 'hotspots' users will be prompted to accept terms and conditions.
[104] *In the Matter of ASUSTeK Computer Inc* FTC Dkt No C-4587 (Jul 28, 2016) (consent order) revealed how security vulnerabilities in the ASUS router and cloud exposed home networks to the interception of data by hackers.
[105] Liu at 3.
[106] Electronic Communications Act 36 of 2005 (ECA), s 1 read with Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 of 2002 (RICA).
[107] See further discussion of the term 'electronic communications service provider' and its application to mobile app developers in chapter 5 and 6.
[108] Federal Trade Commission, *Mobile Security Updates: Understanding the Issues* (attachment A).
[109] The device manufacturer may outsource the actual manufacturing to an OEM (also known as original device manufacturer (ODM)). See e.g. *In the matter of BLU Products and Samuel Ohev-Zion* FTC Dkt No C-4657 (Sep 10, 2018) (consent order). Blu is a brand of smartphone sold in the US. Blu is the device manufacturer but contracted with OEMs to manufacture, customise and brand the devices to Blu's specification.
[110] Smartphones operate on micro-chip processors to enable central processing, memory, input/output ports, storage and radio frequency signal processing. A 'system-on-a-chip' 'is an integrated circuit' combining some or all of these functions onto one chip. See Wikipedia, 'System on a Chip' <https://en.wikipedia.org/wiki/System_on_a_chip> accessed 28 February 2020. A 'chipset manufacturer' is thus 'the entity that provides a mobile computing device's system-on-a-chip, radio chip, or other chipset'. Federal Trade Commission, *Mobile Security Updates: Understanding the Issues* (attachment A).
[111] Cavoukian and Prosch at 10 recommend that devices should be shipped with such features turned off. Users must be clearly informed why if, for regulatory reasons (such as emergency services) or technical reasons, the functionality remains partly active.

installed mobile apps, which directly calls into question their responsibility for user privacy. In 2013 the FTC took action against device manufacturer HTC on this basis,[112] and in a related court settlement, software developer Carrier IQ, HTC and ten other device manufacturers settled a class action law suit[113] brought on the grounds that the 'hidden' app[114] the purpose of which was to diagnose network faults, intercepted sensitive data such as location and communications content. In 2018 the FTC reached a similar settlement with another device manufacturer, Blu.[115] Both cases illustrate that a responsible party cannot abdicate responsibility to a service provider and must perform due diligence when appointing service providers.

---

[112] *In the Matter of HTC America Inc.* FTC Dkt No C-4406 (Jul 25, 2013) (consent order). The case resulted in a consent order which would see HTC subject to biennial audits for the next 20 years to verify adherence to improved security measures agreed in the settlement. HTC had customised the Android and Windows Phone OS on its devices and pre-installed applications (which the user could not uninstall) such as its custom voice-recorder. These apps by-passed the OS permission-based security model and created a security vulnerability that could be exploited to give the same permissions to malicious applications. In addition, Carrier IQ, a 'networks diagnostics' app, was pre-installed on HTC (and other) devices to provide network and device fault reports to network providers Sprint Mobile and AT&T. Through a custom HTC software interface the app was able to access large amounts of sensitive data on the device. Insecure communications allowed malicious apps to communicate with the CIQ interface. Further HTC's failure to deactivate debugging code before shipping devices meant this sensitive information was sent to HTC and stored in system logs (where it was accessible to third party applications with permission to access the system log). The information included GPS-based location information; web browsing and media viewing history; the size and number of all text messages; the content of each incoming text message; the names of applications on the user's device; the numeric keys pressed by the user; and any other usage and device information specified for collection by certain network operators were stored. Further on Android devices it was possible to send text messages which could be used in a toll fraud scheme to subscribe to paid services without the user's knowledge as the SMS would not appear on the device. These details appear in the compliant available at https://www.ftc.gov/sites/default/files/documents/cases/2013/07/130702htccmpt.pdf accessed on 25 February 2020.

[113] *In re Carrier IQ, Inc. Consumer Privacy Litigation*. Full details of the case and settlement are available at http://www.carrieriqsettlement.com/case-documents.aspx, accessed on 25 February 2020.

[114] Removal of the app required accessing the device 'root'. An ordinary user would be unaware that the app was installed and running in the background on the device, and users were not notified of its existence or given any means of uninstalling it.

[115] *In the matter of BLU Products and Samuel Ohev-Zion.* Blu devices were shipped with pre-installed software supplied by a Chinese software developer, ADUPS Technology Co. Ltd. Blu had contracted ADUPS to supply data mining and firmware-over-the-air (FOTA) software to enable Blu to monitor device functioning and deliver OS updates and security patches to its devices. ADUPS in fact collected personal information from users in the US and transferred this to its servers in China. Text message communications content was uploaded every 72 hours (along with call and text message logs and contact lists) and real-time cell tower location data was uploaded every 24 hours. The FTC found Blu deceived customers because its assurance that it implemented appropriate security measures to protect consumer's personal information was false. It failed to implement such measures by failing to conduct an adequate risk assessment on third party software and failing to vet service providers and use contractual measures to require service providers to adhere to data security standards, policies, procedures or practices.

(g) Online Social Network (OSN) Platforms

The term 'online social networks' is used here to describe social networking services, such as Facebook, Twitter and LinkedIn, but also includes content sharing sites such as YouTube, and electronic communication services, such as WhatsApp.[116] These services are hugely popular in their own right, and available as mobile applications (in addition to being accessible via a web browser). However, the full reach of OSNs lies in the ability of other applications to integrate with the OSN (for example, for app login credentials, and for in-app communication and content sharing).

The primary parties in an OSN are the user, being the individual using the service, and the OSN service provider, being the company that makes the OSN platform available.

OSNs have fundamentally changed the role of the user, from one of passive consumption of publisher-curated content, to an active creator and curator of content in direct communication with other users.[117] This in turn has driven a move by online advertisers to site-specific targeted advertising made possible by the personal information associated with a user's profile,[118] and advertising revenue funds the OSN service.[119]

OSNs can be integrated into applications for sign-on using social network login credentials, to allow apps to access user information or to facilitate in-app advertising. For example, Facebook has several SDKs which allow app developers to integrate Facebook APIs into their apps.[120] For users, the login with Facebook API provides an easy app login method, but it also gives apps the ability to view a user's public profile, email address and friends list. Apps can also request permission to make posts to a user's Facebook page. The Facebook API was originally highly privacy-invasive as by default, before changes instituted in 2015 with the migration to Graph API v2.0, developers could access the user's profile, email address, location, likes and friends list, as well as the profile of their friends.[121] It was on this

---

[116] Liu at 1, and 7–8.
[117] Ibid.
[118] Ibid.
[119] Ibid.
[120] Ibid at 9.
[121] Changes in the Facebook graph API and marketing API are documented at Facebook for developers, 'Changelog archive' <https://developers.facebook.com/docs/graph-api/changelog/archive/> accessed 26 February 2020. Facebook's app review process now screens apps more stringently.

basis that the 'designmylife' app, notoriously exploited by Cambridge Analytica for President Trump's election campaign, was able to obtain the raw data from both original survey respondents' Facebook accounts, and the accounts of their friends: some 87 million Facebook users' profiles and likes were processed using its algorithms to predict political affiliations.[122]

OSNs also integrate with ad networks for the delivery of targeted adverts. For example, Facebook permits advertisers to target adverts based on user demographics (although its privacy terms state that it shares anonymous information only and does not disclose any user's identity to advertisers).[123]

[122] Alex Hern, 'Cambridge Analytica: How Did It Turn Clicks into Votes?' *The Guardian* (6 May 2018) <https://www.theguardian.com/news/2018/may/06/cambridge-analytica-how-turn-clicks-into-votes-christopher-wylie> accessed 26 February 2020.
[123] *In re Zynga Privacy Litigation* 750 F3d 1098, 1105-06 (9th Cir 2014).

TABLE 2 FACEBOOK'S TARGETING PARAMETERS MADE AVAILABLE TO ADVERTISERS

Basic Fields	**Parameters/Examples**
Location	Country, State, City, Postal code
Gender	Male, Female, All
Age	Range (from 13–65)
Precise Interest	Travel, Science, Music, …
Broad Category	Cooking, Gardening, iPhone 5, …
Interested In	Male, Female, All
Relationship Status	All, Single, In a relationship, Married, Engaged, Not specified
Language	English, Spanish, French, …
Education	Anyone, In high school, In College, College Grad
Workplaces	Google, Facebook, AT&T, …

Source: Liu (2016) at 10.

In addition, Facebook operates as a platform service that allows developers to design applications that run in Facebook.[124] This may be an additional method for developers to obtain user information and share it with advertisers, contrary to user privacy settings.[125] The term 'frictionless sharing' is used in this context to describe the practice of automatically posting directly from the app to another app or a user's social network profile.[126] In terms of a consent order reached in 2012 with the FTC, Facebook agreed to implement stronger privacy controls within its platform, but in 2019 it consented to a civil penalty of $5 billion and ancillary relief including the creation of an independent privacy board which will oversee, inter alia, that Facebook oversees compliance with the Facebook privacy policy by apps on

[124] Ibid. Zynga develops 'social games', such as Farmville, which are played by millions of Facebook users.
[125] Ibid at 1102. Zynga's social gaming apps such as Farmville were programmed to collect the user's Facebook ID and the referrer header of the website open in the user's browser when they clicked the Zynga game link (from which the user's profile page could be located) and transmit this information to third party advertisers.
[126] The practice cause a public outcry in 2011 when the Spotify music app automatically posted song playlists on a user's Facebook newsfeed.

its platform.[127] This order is a remarkable judicial development indicating that regulators will hold platforms accountable.

V THIRD PARTIES IN THE MOBILE APPLICATIONS ECOSYSTEM

The term 'third party' is used in this dissertation to describe a range of companies the services of which are integrated into the app, or who may receive data from the app. However, while the term is used loosely here, and in some of the literature on app data sharing, the discussion in chapters 4, 5 and 6 will show that for the purpose of assigning legal accountability, the term 'third party'[128] must be distinguished from an operator (processor/service provider) that handles personal information *only* on behalf of, and subject to a written contract with, the responsible party.[129] By contrast, a true third party processes personal information for its own purposes and is not under the direct authority of the party that collected and shared the information.

---

[127] Key requirements set out in the consent order are that:
'1. Facebook must exercise greater oversight over third-party apps, including by terminating app developers that fail to certify that they are in compliance with Facebook's platform policies or fail to justify their need for specific user data;
2. Facebook is prohibited from using telephone numbers obtained to enable a security feature (e.g., two-factor authentication) for advertising;
3. Facebook must provide clear and conspicuous notice of its use of facial recognition technology, and obtain affirmative express user consent prior to any use that materially exceeds its prior disclosures to users;
4. Facebook must establish, implement, and maintain a comprehensive data security program;
5. Facebook must encrypt user passwords and regularly scan to detect whether any passwords are stored in plaintext; and
6. Facebook is prohibited from asking for email passwords to other services when consumers sign up for its services'.

[128] Protection of Personal Information Act 4 of 2013 (POPIA) does not define the term. Cf Children's Online Privacy Protection Rule, 16 C.F.R part 312 (COPPA Rule) §312.2, The California Consumer Privacy Act of 2018, Cal. Civ. Code §§ 1798.100 - 1798.199 (CCPA) §1798.140, and Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA OJ L 119, 4.5.2016 (EU General Data Protection Regulation; GDPR) art 4(10).

[129] POPIA s 1 defines such party as an 'operator'. GDPR art 4(8) defines such party as a 'processor'. CCPA and COPPA Rule 16 C.F.R §312 use the terms business and operator respectively to mean the 'responsible party'. They do not define a party to whom processing is outsourced but clearly permit sub-contracting for this purpose.

(a) Back-end Service Providers

To function, mobile apps rely on a variety of services at the 'back-end'[130] including: data storage,[131] file storage[132] and sharing,[133] notifications, including push notifications,[134] messaging and chat functions, integration with social networks, payment gateways, location services, user management,[135] running business logic,[136] managing database persistence,[137] capacity scaling,[138] real time data synchronisation,[139] and database queries.[140] Monitoring and maintaining the application also requires back-end services: principally app crash analysis,[141]

[130] In the distributed client-server mobile architecture model, the 'front-end' faces the client (i.e. the smartphone user) and the 'back-end' refers to processes performed on data on the server in the data access layer. Google LLC., 'Mobile app backend services' (13 May 2019) <https://cloud.google.com/solutions/mobile/mobile-app-backend-services> accessed 26 October 2019.

[131] Known as object storage this refers to the storage of data, and associated metadata under a unique identifier. Object storage has made cheap, virtually limitless storage (as to quantity and time) possible in 'cloud' data centres such as Amazon Web Services' Netapp and Microsoft Azure. See generally Netapp, 'Object Storage vs. File Storage vs. Block Storage' <https://www.netapp.com/us/info/what-is-object-storage.aspx> accessed 13 April 2020.

[132] Ibid.

[133] Ibid.

[134] See generally Android Developers, 'Notifications Overview' (27 December 2019) <https://developer.android.com/guide/topics/ui/notifiers/notifications> accessed 13 April 2020. A notification is a message, such as a reminder, that is displayed to app users outside the app UI (i.e. the push notification will display on the user's device even if they are not using the app). They can tap on the notification to clear it or take action. Unlike a text message (SMS) it is not sent via a cellular service provider.

[135] This relates both to user authentication (which in turn requires registration and password management, or integration of a third party login API such as login with Facebook or Google) and management of user data.

[136] Backend logic, i.e. the rules that determine how data is created, stored and changed.

[137] In simple terms data is persistent when it needs to be stored permanently (either as static data, or as dynamic data which can be updated with additional data, for example, a user's preference settings. A process is persistent when it needs to continue running despite other processes being closed or a crash.

[138] While this term has technical applications related to network architecture and algorithms used in programming the app, at its simplest scalability refers to the ability of the application to manage increased demand. For a simple explanation, see Techopedia, 'Scalability' <https://www.techopedia.com/definition/9269/scalability> accessed 13 April 2020.

[139] This permits a user to access the service on multiple devices. See Techopedia, 'Data Synchronisation' <https://www.techopedia.com/definition/1006/data-synchronization> accessed 13 April 2020.

[140] In simple terms, a 'query' refers to the retrieval of data from storage using syntax 'understood' by the database (e.g. Structured Query Language or SQL) and its presentation in a format that humans can read. Techopedia, 'What is a query?' <https://www.techopedia.com/definition/5736/query> accessed 13 April 2020.

[141] See Techopedia, 'What does crash mean?' <https://www.techopedia.com/definition/13399/crash> accessed 13 April 2020. A 'crash' in this context refers to an event that causes the application to stop functioning correctly. It is imperative that app developers can detect, find and fix the underlying causes of crashes in order to provide the app user with the most efficient and least frustrating experience.

fraud detection,[142] security testing and server maintenance. Another way of describing 'back-end' services is 'internal support functions'.[143]

(b) Analytics Companies

Mobile app analytics are an essential part of successful app development. The analysis of how users interact with the app permits developers to improve the app by removing defunct features, adding useful features and improving existing features.[144] The analysis allows segmentation of users by demographics, location or device type, and provides the app developer with statistics on, for example, active users, user engagement, app events,[145] session length,[146] revenue,[147] adoption and acquisition channels,[148] and user retention.

Analytics enables developers to 'identify' their most valuable users.[149] Where this is in the form of aggregated statistics about a defined 'audience', or 'segment' the information may still be personal information where it can reasonably be linked with other information to identify a particular individual. On this aspect, industry literature about how analytics providers use personal information is obscure, but a recent study on 300 apps and

---

[142] E.g. identifying the device on which an app was downloaded can prevent a user from trying to sign on to a free trial period multiple times, or an unauthorised person from trying to sign on to the app from a different device.

[143] COPPA Rule 16 C.F.R §312 §312.2 expressly defines '[s]upport for the internal operations of the Web site or online service':

'(1) Those activities necessary to:

(i) Maintain or analyze the functioning of the Web site or online service;

(ii) erform network communications;

(iii) Authenticate users of, or personalize the content on, the Web site or online service;

(iv) Serve contextual advertising on the Web site or online service or cap the frequency of advertising;

(v) Protect the security or integrity of the user, Web site, or online service;

(vi) Ensure legal or regulatory compliance; or

(vii) Fulfill a request of a child [i.e. app user] as permitted by §312.5(c)(3) and (4);'

[144] Hady ElHady, 'Guide to Mobile App Analytics' <https://instabug.com/blog/mobile-app-analytics/> accessed 26 October 2019.

[145] Ibid. A 'conversion event' would be key actions the developer wishes to track such as whether users open the app for the first time (after download) of complete a tutorial. Some app events are automatically captured such sign up or login and ad views or clicks. E-commerce apps would want to capture items viewed, added to carts or proceeding to checkout.

[146] Ibid. E.g. total daily time spent by users in the app, time taken to complete a game level, or sessions taken before making an in-app purchase.

[147] Ibid. Revenue per user or per paid user.

[148] Ibid. While app version has been adopted and where it was downloaded.

[149] Ibid.

eight analytics libraries has demonstrated that personal information is transferred to analytics libraries without user notification.[150]

(c) Data Brokers

Data broking is a large and lucrative international industry,[151] but its practices, which are shrouded in a degree of secrecy, have raised privacy concerns.[152] Data brokers (or information brokers, data providers or data suppliers) are companies that collect personal information on individuals.[153] They buy information (for example, from credit card companies) and aggregate that with information obtained both online and offline, such as web and purchase history, age, gender and income bracket,[154] in order to sell audience segments to marketers.[155]

Although the information may be obtained from public sources,[156] it is doubtful whether the consumer has given specific, informed consent for such collection, and the legitimate interests of data brokers and advertisers must be balanced against the right to privacy of the data subject. The practices of data brokers highlight the need for clarity on the definition of personal information in two respects. First, are device identifiers and online aliases (not personal identity names and numbers) personal information? Second, is the derived data (predictions and inferences based on the facts collected) also personal information? The definition of personal information will be considered in chapters 4, 5 and 6.

---

[150] Xing Liu and others, 'Privacy Risk Analysis and Mitigation of Analytics Libraries in the Android Ecosystem' (2019) 19 *IEEE Transactions on Mobile Computing* 1184–1199.

[151] Michal Wlosik, 'What Is a Data Broker and How Does It Work?' (23 January 2019) <https://clearcode.cc/blog/what-is-data-broker/> accessed 26 October 2019. They include subsidiaries of large corporates such as Oracle, and credit reporting agencies Experian and Equifax. They also include people-search sites such as www.PeekYou.com, and www.Spokeo.com.

[152] Privacy International, 'Why we've filed complaints against companies that most people have never heard of – and what needs to happen next' (8 November 2018) <https://privacyinternational.org/advocacy/2434/why-weve-filed-complaints-against-companies-most-people-have-never-heard-and-what> accessed 26 October 2019. Also see e.g. Kashmir Hill, 'Data Broker Was Selling Lists Of Rape Victims, Alcoholics, and 'Erectile Dysfunction Sufferers'' (19 December 2013) <https://www.forbes.com/sites/kashmirhill/2013/12/19/data-broker-was-selling-lists-of-rape-alcoholism-and-erectile-dysfunction-sufferers/#6ab63ca71d53> accessed 26 October 2019.

[153] Wlosik.

[154] Ibid.

[155] Ibid.

[156] Ibid. E.g. public social media profiles or from companies that you disclosed your information to (and consent to share your information with a data broker was included in in the 'fine print' of the terms and conditions).

(d) Advertising Networks

'In-app' adverts are the primary source of revenue for free to download ('fremium') apps.[157]

The term 'mobile in-application advertising' means 'an advertisement displayed within a mobile application. It can be displayed on the mobile device's screen as a banner at the top or bottom of the screen, mobile interstitial or as an overlay ...'.[158] Banner ads appear as flyers at the top or bottom of the screen.[159] Overlays or native ads appear as small ads within the user interface.[160] Interstitials appear as whole screen adverts,[161] including reward videos, where users earn app 'currency' for viewing the ad.[162] As described further below, much of this advertising is now highly targeted – meaning that an ad will be delivered to a user if, based on personal information collected about that user, the ad is viewed as 'relevant' to their interests. The term 'ad tech' refers to 'tools that analyse and manage information (including personal data) for online advertising campaigns and automate the processing of advertising transactions'.[163]

In-app advertising is implemented via a third party ad network, which raises privacy concerns around the identity of the third parties involved, the nature of the information they have access to, and how that information is monetised through advertising and other uses. At its simplest, there are four parties involved in the mobile app advertising ecosystem:[164]

Users: These are the individuals who are using the app on a smartphone, and who are a potential target of advertisers.

Advertisers: These are the companies marketing their product through adverts, with the assistance of a digital advertising agency. Advertisers will determine,

---

[157] Typically, developers will make a lightweight version of the app available for free, but 'premium' features can only be accessed with an in-app purchase or subscription. J Clements, 'Distribution of worldwide mobile application revenues in 2017, by channel' (20 Feb 2018) <https://www.statista.com/statistics/273120/share-of-worldwide-mobile-app-revenues-by-channel/> accessed 24 October 2019.

[158] International Telecommunications Union Standardisation Sector (ITU-T).

[159] Google Ad Manager, 'Mobile Ads SDK Android Guide' <https://developers.google.com/ad-manager/mobile-ads-sdk/android/quick-start> accessed 24 October 2019.

[160] Ibid.

[161] Ibid. Also see Google Ad Manager Help, 'How mobile app interstitials work' <https://support.google.com/admanager/answer/6015986?hl=en> accessed 24 Oct 2019.

[162] Ibid. Also see Google Ad Manager Help, 'Rewarded inventory policy' <https://support.google.com/admanager/answer/7496282> accessed 24 October 2019.

[163] Information Commissioner's Office (UK), *Update Report into AdTech and Real Time Bidding* (2019) at 8.

[164] These terms are described generally. For further detail see IAB.

based on the campaign budget, what amount they are prepared to pay per impression (CPM)[165] or per click (CPC).[166] They will also decide on targeting parameters, designed to make the advert more effective by reaching a receptive audience.

Publishers: These are the app developers who have joined the ad network. Developers earn revenue based on the number of 'impressions' displayed or on the number of 'clicks' generated within their app, paid by advertisers, from which ad networks take a commission.

Ad-network: This is the company acting as an intermediary through which users, advertisers and publishers can be connected. An example is Google AdMob.[167]

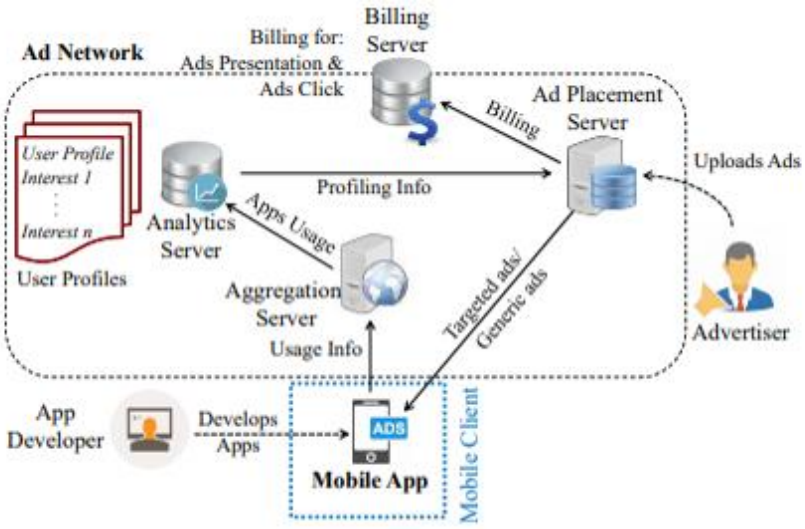
Figure 2.1 illustrates the information flow between the different parties. Advertisers upload ads to the ad server owned by the ad network. Information is transferred from the app to the ad network's servers where it is aggregated and analysed to develop a user profile against which targeted advertisements can be delivered, for which the advertiser is then billed for the number of times the ad is served to users (ad impressions) or the number of clicks on the ad.[168]

To permit this functionality, the app must incorporate the ad library – code (written by the ad network)[169] that enables the app to communicate information from the app to the advertising server and to retrieve and display advertisements. When code is packaged within a set of software tools, it is called a software development kit (SDK). For example, a developer working with Google Ad Manager would incorporate the Google Mobile Ads SDK[170] to serve in-app advertising. But a developer can also integrate several third-party ad networks, which include Google's AdMob, Facebook's Audience Network and Flurry. This

[165] Cost-per-mile, or cost per 1000 impressions, an impression being the number of times an ad is displayed/presented to a user.
[166] Cost per click. For a general description of how online advertising works, and the pricing mechanism in the traditional web environment and the OSN environment see Liu at 10–11.
[167] Google AdMob is examined in depth in Imdad Ullah, 'Privacy-preserving mechanisms for targeted mobile advertising' (University of New South Wales, Sydney, Australia 2017).
[168] Ibid.
[169] The code may be proprietary or open source. See e.g. the list of ad networks that can be mediated through the Google Mobile Ads SDK in Google Ad Manager.
[170] Ibid.

is done by incorporating the Google Mobile Ads SDK, along with the ad network's SDK and an adapter library – code that enables communication between Google AdExchange and the networks, which then bid for advertising space within apps.[171]

FIGURE 1: THE IN-APP ADVERTISING ECOSYSTEM, INCLUDING THE INFORMATION FLOW BETWEEN DIFFERENT PARTIES



Source: Ullah (2017)

The developer may not be aware of the personal information that will be collected by the advertising network. However, it is unlikely that the app developer would escape liability because, as a responsible party, the app developer must arguably take reasonable steps to verify the data-handling practices of third party code it embeds in the app.[172]

The ad network may incur direct liability to consumers. In February 2019, Kiip, an advertising network that offered in-app reward-based advertising in over 4 000 apps, settled a class action law suit (without admission of liability) related to its collection and use of personal information about app users.[173] The practice came to light when the Norwegian

[171] Ibid.
[172] This is discussed further in chapters 4, 5 and 6, and recommendations for reform in South Africa are proposed in chapter 9.
[173] Complaint filed on 21 October 2016 in *Vasil v Kiip Inc.* No 16-CV-09937 (ND Ill Mar 5, 2018), consolidated with *Farag et al v Kiip Inc.* No 2019 CH 01695 (Ill Cir Ct Cook Cnty Oct 18, 2019) (settlement order). A modest $1 million settlement was reached: 'Farag v Kiip Settlement' <https://www.kiipsettlement.com/> accessed 26 February 2020. Kiip has subsequently filed for bankruptcy and been bought by NinthDecimal, a larger digital marketing company: Leo Kangin, 'Interview with Brian Wong' (*Brief Communications Inc*, 2019) <https://gobrief.com/interviews/kiip-with-brian-wong/> accessed 15 May 2020. For NinthDecimal's approach

Consumer Counsel identified that the Runkeeper app was transmitting user location data to Kiip even when the app was not in use.[174] Runkeeper's sharing of personal information with advertisers is by no means unique.[175] It is clear that despite self-regulatory efforts by a number of industry organisations,[176] there remains room for concern.

(e) Advertising Exchanges

An ad exchange moves one step beyond an ad network by providing a technological platform (or 'marketplace') for real-time bidding by advertisers (buyers) for ad inventory[177] made available by participating publishers (sellers).[178] In simple terms, an ad exchange simultaneously connects multiple publishers and multiple ad networks, and auctions advertising inventory based on algorithms to determine the winning bid. However technology has advanced to the point where the ad exchange may be integrated with demand side platforms (DSPs) that permit advertisers to manage multiple ad exchange accounts, and supply side platforms (SPSs) that permit publishers to manage advertising inventory with multiple advertising partners.[179] Ad serving is the 'on-demand' process of selecting an ad to display to the user.[180] The app will communicate an ad request to the ad server and information required to respond to that request.[181]

---

to privacy and membership of industry associations, see NinthDecimal, 'Consumer and Data Privacy' <https://www.ninthdecimal.com/> accessed 26 February 2020.

[174] Runkeeper subsequently cut ties with Kiip and issued a public apology as part of it commitment to work with the Norwegian data regulator to address security and privacy issues. Jason Jacobs, 'A Message to Our Users ' (*Runkeeper Blog*, 17 May 2016) <http://blog.runkeeper.com/4714/a-message-toour-users/> accessed 26 February 2020.

[175] For further details of the Norwegian Consumer Councils investigations into other mobile app data-sharing practices, see ForbrukerRåder (Norwegian Consumer Council), '#AppFail' <https://www.forbrukerradet.no/appfail-en/#> accessed 26 February 2020.

[176] These include the Digital Advertising Alliance, the Network Advertising Initiative, the US Media Rating Council, the Advertising Research Foundation (ARF), Mobile Marketing Association (MMA) and the Interactive Advertising Bureau (IAB). In South Africa the South African Advertising Research Foundation (SAARF) is a member of both the US AFR and the European Media Research Organisation, and the IAB has a South African chapter. Available at https://www.mediaupdate.co.za/marketing/16760/sa-advertising-research-foundation, accessed on 26 February 2020. The IAB (https://www.iabsa.net/home/, accessed on 26 February 2020) and the MMA (https://www.mmaglobal.com/local-council/south-africa, accessed on 26 February 2020) also have South African chapters.

[177] Effectively the ad 'space' in an app.

[178] The top ad exchanges include AppNexus, AOL's Marketplace, Index Exchange, Microsoft Ad Exchange, OpenX, Rubicon Project Exchange, Smaato and Google AdExchange (formerly DoubleClick). See 'Ad Exchange' <https://en.wikipedia.org/wiki/Ad_exchange> accessed 24 Oct 2019.

[179] Ibid.

[180] Ryan Stevens and others, 'Investigating User Privacy in Android Ad Libraries' in *Workshop on Mobile Security Technologies (MoST)*, vol 10 (Citeseer 2012).

[181] Ibid.

VI DATA PROCESSING IN THE MOBILE APPLICATIONS ECOSYSTEM

(a) Data

The term 'data' can be understood differently in different contexts. In the disciplines of Information Systems, Computer Science and Software Engineering, the term 'data' can be understood in different ways. In one sense, data refers to the inputs into a computer system, represented in the signs and symbols of the programming code. In a second sense, data represents facts understandable to humans:

> *'Data: Natural language: facts given, from which others may be deduced, inferred. Info: Processing and computer science: signs or symbols, especially for transmission in communication systems and for processing in computer systems, usually but not always representing information, agreed facts or assumed knowledge; and represented using agreed characters, codes, syntax and structure.'*[182]

The use of the term 'data' in a legal context should be approached with caution. The term 'data' in this context is equivalent to 'information', and the terms 'personal data'[183] or 'personal information'[184] broadly mean data that identifies an individual (or from which an individual can be identified). It excludes anonymised or de-identified data. It includes pseudonymised or aggregated data to the extent that there is a reasonable possibility of an individual being identified (or re-identified) when the pseudonymised or aggregated data is combined with other data.

(b) Metadata

Metadata (which in some contexts may be called traffic data[185]) is distinguished from content data. When a user interacts with an app, for example, to upload photos, watch a video, or send

---

[182] Peter Checkland and Sue Holwell, 'Data, capta, information and knowledge' in Matthew Hinton (ed), *Introducing Information Management* (Routledge 2006) at 48, quoting Maddison, R (ed), *Information Systems Development for Managers* (Paradigm 1989) at 174. Also see International Electrotechnical Commission (IEC) at 171-01-02 defines 'data' as a 'representation of information in a formalized manner suitable for human or automatic processing' and at 171-01-01 defines 'information' as 'knowledge concerning objects, such as facts, events, things, processes, or ideas (including concepts) that, within a certain context, has a particular meaning.'

[183] GDPR art 4(1). As to the terms 'data' and 'information' see further Anneliese Roos 'Data Protection' in Van der Merwe D (ed) *Information and Communications Technology Law* (2 ed, LexisNexis 2016) at 368, specifically footnote 35.

[184] POPIA, s 1; CCPA; and Children's Online Privacy Protection Act of 1998, 15 U.S.C. §§ 6501 - 6506 (2018) (COPPA). In South Africa the term includes information about juristic persons.

[185] Traffic data is specifically the metadata about communications 'traffic' over a cellular or internet network. This may include 'data referring to the routing, duration, time or volume of a communication, to the protocol

a message the photo, video or text is content data.[186] However, there is also a great deal of metadata about this content: 'information about the item's creation, name, topic, features, and the like'.[187] By way of analogy, in an offline context, while the text of the book is content, the bibliographic information recording the author, publisher, subject area and ISBN number is metadata.[188] As this simple example illustrates, the boundary between the two concepts can be indistinct, since metadata can also tell us important information from which we can infer a great deal about the content of the book.[189]

In the same way, while the confidentiality of the content of communications is clearly inherent in the protection of privacy,[190] the metadata about electronic communications (such as numbers called, browsing history, location, call time, date and duration) permit 'precise conclusions to be drawn regarding the private lives of persons involved in the electronic communication, such as their social relationships, their habits and activities of everyday life …'.[191] Case law in the US[192] and the EU[193] supports the view that collection of

---

used, to the location of the terminal equipment of the sender or recipient, to the network on which the communication originates or terminates, to the beginning, end or duration of a connection, …[or the] format in which the communication is conveyed by the network.' e-Privacy Directive 2002/58/EC art 2(b) and rec 15.

[186] See e.g. Europe *Von Hannover v. Germany (no. 2)* [GC], nos 40660/08 and 60641/08, ECHR 2012 where the European Court of Human Rights recognised a privacy interest in the name, image and likeness of a public figure. For the earliest decision in South Africa on the privacy of photographs see *O'Keeffe v Argus Printing and Publishing Co Ltd and another* 1954 (3) SA 244 (C) and the discussion in Anneliese Roos, 'Privacy in the Facebook Era: A South African Legal Perspective' (2012) 129 *SALJ* 375–402 at 377 and South African Law Reform Commission, *Project 124 'Privacy and data protection'* (2009) at 22.

[187] Jenn Riley, 'Understanding Metadata: What is Metadata, and What is it For?: A Primer' (*National Information Standards Organisation (NISO)*, 2017) <https://www.niso.org/publications/understanding-metadata-2017> accessed 26 October 2019.

[188] Ibid.

[189] Ibid.

[190] *S v A and another* 1971 (2) SA 293 (T); *Financial Mail (Pty) Ltd v Sage Holdings Ltd and Another* 1993 (2) SA 451 (A) at 463. As to the person, place and relationship-orientated aspects of the privacy right see generally *Bernstein and others v Bester and others NNO* 1996 (2) SA 751 (CC) para 65, and specifically the discussion in fn 89.

[191] Proposal for a regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic
communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) Brussels, 10.1.2017 COM(2017) 10 final 2017/0003 (COD) rec 2.

[192] *Carpenter v United States* 585 US (2018), overturning *United States v Carpenter* 819 F3d 880 (6th Cir 2016). The US Supreme Court held by a narrow 5:4 majority that obtaining historical cell-site location information (CSLI) without a warrant violated 4th amendment rights. Also see *United States v Jones* 565 US 400 (2012) which relied on concept of trespass to find that affixing a GPS tracker to a car violated the 4th amendment. The majority judgment does not address whether GPS-based location tracking that does not involve a physical trespass (e.g. using data from a mobile phone) is protected. It should be noted that there is no reported decision in South Africa concerning the use of location data, whether it be GPS location data or cell site location information.

[193] *Vorratsdatenspeicherung [Data retention]* 125 BVerfGE 260 (2010) [English translation available at <https://wwwbundesverfassungsgerichtde/entscheidungen/rs 20100302_1bvr025608html> accessed on 27 July

metadata can constitute a privacy invasion. It has also been recognised that the capacity to store and transmit metadata poses a heightened risk to the right to privacy in the digital age.[194]

(c) Location Data

Location data means data that reveals the geographic position of the user's device,[195] and is expressly included in the definition of 'personal information'.[196] There are a number of ways location data can be collected. First, the on-device GPS sensor enables location tracking which is accurate to 1.5 metres (five feet).[197] An app user has some control over location tracking as they must grant an app permission to access location and can also turn off location services in the device system settings.[198] Photographs taken with the device camera can be embedded with a geo-tag of the location, date and time when the photograph was taken and unless this setting is also disabled, the user's location is accessible to any party that receives the photograph.[199]

Secondly, network-based location, or cell site location information (CSLI), refers to a form of location tracking enabled by the continuous connection of the cell phone

---

2019] . The principle of proportionality was invoked by the German Federal Constitutional Court to strike down German national laws implementing the EU Data Retention Directive, which permitted retention for six months of communication 'traffic data': Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC OJ L105, 13.04.2006. See further Katja De Vries and others, 'The German Constitutional Court Judgment on Data Retention: Proportionality Overrides Unlimited Surveillance (Doesn't It?)' in Serge Gutwirth and others (eds), *Computers, Privacy and Data Protection: an Element of Choice* (Springer Netherlands 2011) and the further cases referred to therein.

[194] *M.L. and W.W. v Germany* no 60798/10 and 65599/10, ECHR, 2018 para 91 and the further cases cited therein. The case concerned an unsuccessful attempt to be 'forgotten online' by having historic news articles anonymised. As such it also concerns the balance between the right to privacy and the competing rights of journalists to freedom of expression and the public's right of access to information.

[195] See e.g. the definition in the e-Privacy Directive 2002/58/ECart 2(c) and rec 14: 'any data processed in an electronic communications network, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service'.

[196] POPIA s 1, GDPR art 4(1), COPPA Rule 16 C.F.R §312.2 and CCPA §1798.140(o).

[197] National Association of Criminal Defense Lawyers (NACDL), 'Cell Phone Location Tracking' <https://www.law.berkeley.edu/wp-content/uploads/2015/04/2016-06-07_Cell-Tracking-Primer_Final.pdf> accessed 26 July 2019.

[198] Questions remain over whether these settings are observed. E.g. On Google's collection of time stamped location despite location settings being turned off see Ryan Nakashima, 'Google tracks your movements, like it or not' (*Associated Press*, 14 August 2018) <https://apnews.com/828aefab64d4411bac257a07c1af0ecb> accessed 14 April 2020. Also see Elizabeth Williams and Johnathan Yerby, 'Google and Facebook Data Retention and Location Tracking through Forensic Cloud Analysis' in South Association for Information Systems (SAIS) (ed), *SAIS 2019 Proceedings* (2019).

[199] Techopedia, 'Geotagging' <https://www.techopedia.com/definition/86/geotagging> accessed 25 February 2020.

to the cell sites (radio antennae positioned on cell towers or buildings) from which it obtains its signal and on which its functionality depends.[200] The connection automatically generates a time-stamped record.[201] By triangulating the signal, greater accuracy is obtained.[202] Mobile apps can gain access directly to real-time network-based location (and store this for historical analysis) through the OS API if they are granted permission to access location.

Thirdly, when a device is connected to a wireless network (WLAN), BSSID,[203] ESSID[204] and network signal strength can be collected. While developers may need to check if the device is connected to Wi-Fi and even turn Wi-Fi on or off for a particular app functionality, the co-ordinates provided by the BSSID and ESSID, together with signal strength, allow for passive tracking of user location even when location services are not enabled.[205]

The ability of the smartphone to facilitate tracking of the location of an individual has long been subject to regulatory scrutiny, [206] and has been recognised by the US

---

[200] *Carpenter v United States* at 1 (Majority opinion per Roberts, J.).

[201] The term historical CSLI thus refers to this record of past movements, that is automatically being collected and stored about every cell phone user. The term 'real-time' data relates to tracking in the present moment. Access by law enforcement officials to the records stored by MNOs is controlled under RICA in SA, but a discussion of its provisions, and comparison to US and EU legislation governing domestic and cross-border access to data is beyond the scope of this dissertation.

[202] National Association of Criminal Defense Lawyers (NACDL).

[203] The BSSID (basic service set identifier) is the 'address' of a wireless access point (WAP) within a wireless network (WLAN) (it is a 48-bit number or MAC address) through which a data packet must be routed. The term SSID (service set ID) is the unique name given to a WLAN service profile by the WLAN administrator. To the device user SSIDs are displayed as the names of the available Wi-Fi networks recognised by the device. A user would then click on a network name (SSID) (and enter the password if required) to connect to that network. Juniper Networks, 'Understanding the Network Terms BSSID, SSID and ESSID' (5 October 2018) <https://www.juniper.net/documentation/en_US/junos-space-apps/network-director3.7/topics/concept/wireless-ssid-bssid-essid.html> accessed 8 March 2020.

[204] When a WLAN comprises multiple access points the ESSID (extended basic service set ID) is the 'name' of the network and identifies all the BSSIDs in the network. When the user physically moves their device to a different area it will remain connected to the ESSID but the BSSID will change as the connection will be routed via the closest available access point. Ibid.

[205] Gabriella Verga and others, 'Yet Another Way to Gather People Co-ordinates and its Countermeasures' in Raffaele Montella and others (eds), *Internet and Distributed Computing Systems* vol 11874 (IDCS 2019. Lecture Notes in Computer Science, Springer, Cham 2019). Also see *United States v InMobi Pte Ltd* Case No 3:16-cv-03474 (ND Cal Jun 22, 2016).

[206] *In the matter of Goldenshores Technologies, LLC and Erik M. Geidl* FTC Dkt No C-4446 (Apr 9, 2014) (consent order). The 'Brightest Flashlight App' was a hugely popular free app. The privacy policy and end-user license agreement (EULA) represented that the app 'may periodically collect, maintain, process, and use information from users' mobile devices to provide software updates, product support, and other services to users related to the Brightest Flashlight App, and to verify users' compliance with [the] EULA.' In fact, the app was tracking both precise geolocation and persistent device identifiers, and sharing this information with third party advertising networks. The consent order required 'clear and prominent notice' and 'express affirmative consent' from users before collecting geo-location information.

Supreme Court as a privacy invasion as it creates an 'intimate window' into an individual's movements from which other personal information can be deduced.[207]

Operating system (OS) platforms are responding to privacy concerns for greater user control. Android permits app developers to request permissions either to 'ACCESS_FINE_LOCATION' (providing a precise GPS location) or to 'ACCESS_COARSE_LOCATION' (providing an approximate network-based location).[208] However, it remains the responsibility of the app developer to select the minimum level of access required for the functions the app performs,[209] and the permission request will not notify the user whether fine-grained or coarse-grained permission is being requested by the app, or automatically raise a red flag if location is not needed by the app.

(d) Device Fingerprinting (What happened to the cookies?)

A device can be uniquely identified by a combination of publicly-available parameters such as the device name,[210] device type, OS version, connection type and carrier. Device fingerprinting must be distinguished from browser-based tracking technologies, such as cookies[211] and web beacons.[212] Cookies are the most familiar to users and have been widely discussed by regulators and academics. Although cookies and web beacons are not placed inside mobile apps, by fingerprinting the device, trackers can link users across all of their online activity (even if an advertising identifier is reset).

---

[207] *Carpenter v United States* at 12, citing *United States v Jones* at 415, per Sotomayor, J., concurring. Cf *Carpenter v United States*, at 17, per Kennedy, J., dissenting. Despite the breadth of these remarks the decision is a narrow one, finding that criminal investigators require a probable cause warrant to access CSLI and it is insufficient to rely on a court order under the Stored Communications Act of 1986, 18 U.S.C. §§ 2701–2712 (2018).

[208] Android Developers, 'Permissions Overview'. Also see the discussion on background processing.

[209] Android Developers, 'Privacy best practices' (27 December 2019) <https://developer.android.com/privacy/best-practices> accessed 19 February 2020.

[210] E.g. Dusty's iPhone.

[211] Cookies are small encrypted text files stored in the browser that permit tracking of which web pages a user has visited and how they interacted with the site. Cookies are not viruses and they cannot open or access information on the device. In fact some cookies are useful. Session cookies enable a web page to 'remember' where the user was when they last landed on the web page or store items in a shopping cart. Persistent (tracking) cookies can be placed by the web site owner (first party cookies) or by advertisers, analytics companies and other third parties (third party cookies). They can be used to store user preferences (giving a 'customised' or 'personalised' web experience) but they can also be used for profiling all of a user's online activity. See allaboutcookies.org, 'Mobile technology tracking methods other than cookies' <https://www.allaboutcookies.org/mobile/mobile-tracking.html> accessed 3 November 2019.

[212] A web beacon (pixel tracker or web tag) is a clear pixel embedded on a web page or inside an email that permits email senders/web page owners, advertisers, analytics companies and social media networks to track when a user accesses a web page or reads an email.

(e) Data Lifecycle

This refers to the phases through which data passes: 'creation or collection, processing, dissemination, use, storage and disposition, including deletion and destruction'.[213] Under POPIA, the term 'processing' has a wide meaning, which would encompass all of the phases of the data lifecycle, and would apply to any data that is 'personal information'.

(f) Big Data

The term 'big data' refers broadly to very large data sets which are analysed to make predictions or discover new insights. Thus big data analytics 'refers to the whole data management lifecycle of collecting, organizing and analysing data to discover patterns, to infer situations or states, to predict and to understand behaviours'.[214] The emergent importance of big data analytics is powered by advances in the storage and computational capacity of computers.[215] There is no universally accepted comprehensive definition of big data, as big data analytics is a constantly evolving field. It has been defined with reference to: *volume*, referring to the large size of the data sets; *velocity*, referring to real-time analysis of streaming data; and *variety*, referring to the analysis of diverse data from different sources, including structured and semi-structured data, as well as unstructured data such as text, audio and images.[216] Three additional elements have been added to this description: *variability*,

---

[213] Department of Homeland Security (DHS) Privacy Office, *Handbook for Safeguarding Sensitive PII, Privacy Policy Directive 047-01-007, Revision 3* (2017) at 7.

[214] ENISA, *Privacy by Design in Big Data: An Overview of Privacy by Design in the Era of Big Data Analytics* (2015)

[215] An analysis of 'big data' processing lies outside the scope of this dissertation. There is a growing body of recent work on the ethical and privacy implications of big data. See United Nations Development Group (UNDG), *Data Privacy, Ethics and Protection: Guidance Note on Big Data for Achievement of the 2030 Agenda* (2017) Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data ("Convention 108"), *Guidelines on the Protection of Individuals with regard to the Processing of Personal Data in a World of Big Data* (T-Pd(2017)01, 23 January 2017); European Data Protection Supervisor (EDPS), *Opinion 8/2016 on the Coherent Enforcement of Fundamental Rights in the Age of Big Data* (2016). For scholarly criticism of the adequacy of data protection laws see Sandra Wachter, Brent Mittelstadt and Luciano Floridi, 'Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation' (2017) 7 *International Data Privacy Law* 76–99; Mary Madden and others, 'Privacy, Poverty, and Big Data: A Matrix of Vulnerabilities for Poor Americans' (2017) 95 *Wash UL Rev* 53–125, Michael Veale and Reuben Binns, 'Fairer Machine Learning in the Real World: Mitigating Discrimination Without Collecting Sensitive Data' (2017) 4 *Big Data & Society* 1–17, Reuben Binns and others, 'It's Reducing a Human Being to a Percentage': Perceptions of Justice in Algorithmic Decisions' in *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems* (ACM, Montréal, QC 21–26 April 2018) and Mike Ananny and Kate Crawford, 'Seeing Without Knowing: Limitations of the Transparency Ideal and its Application to Algorithmic Accountability' (2018) 20 *New Media & Society* 973–989.

[216] Gartner IT Glossary, 'Definition of Big Data' <https://www.gartner.com/en/information-technology/glossary/bigdata#:~:text=Big%20data%20is%20high%2Dvolume,decision%20making%2C%20

referring both to the variable rate of data flows; *veracity*, referring to the analysis of inherently unreliable data such as human sentiments; and *value*, referring to the high value of analytical insights compared to the relatively low value of the initial data inputs.[217]

Big data is synonymous with mobile applications, which provide a rich source of data, built on the back of powerful mobile cloud computing solutions, which provide the storage and processing capacity necessary to handle the complex analytics.[218]

(g) Data Sharing

The term 'data sharing' is described in some studies[219] with reference to the tracking of mobile app users. 'Trackers' refers to code embedded in the app that permits the transfer of information from the app to third parties, such as analytics and advertising services. Dynamic analysis of traffic flows from the app and static analysis of app code can reveal the presence of trackers.

At a broader level, data sharing (and data selling)[220] can include the practice of aggregating data, and making it available to corporate 'partners' (usually at a price). These business practices may not be disclosed to users and may be shrouded in a degree of secrecy.

---

and %20process%20automation.> accessed 1 August 2020. Also see Amir Gandomi and Murtaza Haider, 'Beyond the Hype: Big Data Concepts, Methods, and Analytics.' (2015) 35 (2) *International Journal of Information Management* 137–144 at 138 &140, and Beverley A. Townsend and Donrich W. Thaldar 'Navigating Uncharted Waters: Biobanks and Informational Privacy in South Africa.' (2019) 35 (4) *South African Journal on Human Rights* 329–350 at 331.

[217] Gandomi and Haider, at 139.

[218] See generally Ibrahim Abaker Targio Hashem and others., 'The Rise of "Big Data" on Cloud Computing: Review and Open Research Issues' (2015) 47 *Information Systems* 98–115 at 100–102.

[219] See e.g. Binns and others, Narseo Vallina-Rodriguez and others, 'Tracking the trackers: Towards understanding the mobile advertising and tracking ecosystem' (1st Data and Algorithm Transparency Workshop, New York, NY, 2016); and Abbas Razaghpanah and others, 'Apps, trackers, privacy, and regulators: A global study of the mobile tracking ecosystem' [2018] <https://www.ftc.gov/system/files/documents/public_comments/2018/08/ftc-2018-0052-d-0036-154997.pdf> accssed 29 October 2019.

[220] Although many privacy policies will claim they do not sell personal information, under the CCPA, the term 'selling' of personal information includes the activities of 'sharing' personal information described here, even if there is no direct monetary payment.

(h) Raw data

Raw data is unprocessed and unstructured.[221] It can be processed ('cooked') to structure, or format, the data into usable information, and in doing so it can also be aggregated, anonymised, pseudonymised or encrypted.

(i) Aggregated data

The term aggregation generally means 'the process of combining things or amounts into a single group or total'.[222] In an online context, this can refer to gathering disparate information from multiple sources,[223] and it is generally used as a statistical term of art to refer to the replacement of individual items of data with summary data represented as a weighting, average or sum (total).[224] Aggregation thus does not guarantee individual anonymity. When a large data set (pertaining to a large number of individuals) is highly aggregated, it may not be possible to link the information to an identifiable individual. However, when data is only partially aggregated or data sets are small, it may be possible to derive personal information about an individual.

(j) De-identified (anonymous) data

Anonymisation is a 'process by which personal data is irreversibly altered in such a way that a data subject can no longer be identified directly or indirectly, either by the data controller alone or in collaboration with any other party'.[225] Simple anonymisation techniques that involve removing direct identifiers such as name, home address or phone number may not yield truly anonymous data. Several studies have shown that it is possible to re-identify an individual with relative ease. For example, anonymised location data with four spatio-temporal points can identify 95% of individuals from their pattern of movements,[226] and

---

[221] Techopedia, 'What is raw data?' <https://www.techopedia.com/definition/1230/raw-data> accessed 13 April 2020.
[222] 'Cambridge English Dictionary' <https://dictionary.cambridge.org/dictionary/english/> accessed 30 March 2020.
[223] Ibid, listing also a second meaning as 'the process of collecting information from several different websites, newspapers, databases (= large amounts of information stored in a computer system), etc. and combining it in one place, or the result of this process.'
[224] OECD, 'Glossary of Statistical Terms' <https://stats.oecd.org/glossary/detail.asp?ID=68> accessed 4 April 2020.
[225] *Information technology — Security techniques — Privacy framework* (ISO/IEC 29100).
[226] Yves-Alexandre De Montjoye and others, 'Unique in the Crowd: The Privacy Bounds of Human Mobility' (2013) 3 *Scientific Reports* 1376. Also see Latanya Sweeney, 'K-anonymity: A Model for Protecting Privacy'

99.9% of individuals in the state of Massachusetts can be correctly re-identified from an anonymised dataset containing only 15 demographic variables.[227]

Data protection legislation is technologically neutral, and thus does not set out the processes by which de-identification is to be achieved.[228] It requires, however, that it must have as its outcome the deletion of any information that identifies the data subject, and that there is no reasonably foreseeable means of reversing the de-identification ('re-identifying' the information), or linking the information to other information and in that way identifying the data subject.[229] This would require an objective enquiry into the likelihood of re-identification or linking based upon all relevant facts.[230]

Data that has been 'de-identified' is anonymous and consequently is no longer 'personal information'. As anonymity is considered a state of privacy,[231] it may be regarded that processing which effectively grants anonymity also protects privacy.

(k) Pseudonymised data (why has my data been hashed?)

Personal information can be protected by removing direct identifiers, and replacing them with an alias (pseudonym).[232] There needs to be separation at a technical and organisational level

---

(2002) 10 *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems* 557–570, Hui Zang and Jean Bolot, 'Anonymization of Location Data Does Not Work: A Large-Scale Measurement Study' in *Proceedings of the 17th Annual International Conference on Mobile Computing and Networking* (ACM, Las Vegas 19–23 September 2011), Arvind Narayanan and Vitaly Shmatikov, 'Robust De-Anonymization of Large Sparse Datasets' in *2008 IEEE Symposium on Security and Privacy (SP 2008)* (IEEE, Oakland CA 18–21 May 2008) and M Keith Chen and Ryne Rohla, 'The Effect of Partisanship and Political Advertising on Close Family Ties' [2017] *arXiv preprint arXiv:171110602*.

[227] Luc Rocher, Julien M. Hendrickx & Yves-Alexandre de Montjoye, 'Estimating the Success of Re-identifications in Incomplete Datasets Using Generative Models' (2019) *Nature Communications* 10:3069 at 5.

[228] It is beyond the scope of this dissertation to discuss the techniques and tools for anonymisation.

[229] POPIA s 1. '"de-identify", in relation to personal information of a data subject, means to delete any information that–

(a) identifies the data subject;

(b) can be used or manipulated by a reasonably foreseeable method to identify the data subject; or

(c) can be linked by a reasonably foreseeable method to other information that identifies the data subject,

and 'de-identified' has a corresponding meaning.'

[230] Also see GDPR rec 26 which provides: 'To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and amount of time required for identification, taking into consideration the available technology at the time of the processing, and technological developments.' The term 'anonymisation' is not defined in GDPR or the other data protection statutes studied.

[231] Alan F. Westin, *Privacy and Freedom* (Athenum 1967) at 34.

[232] Samson Esayas, 'The Role of Anonymisation and Pseudonymisation under the EU Data Privacy Rules: Beyond the 'All or Nothing' Approach' (2015) 6 *European Journal of Law and Technology* 1–28.

of any personal identifiers and the pseudonymised data set.[233] In this way, the information can be used to identify an individual indirectly only if it is possible to link the information to other information that identifies the data subject. GDPR encourages pseudonymisation but it is only one means (and not necessarily always a sufficient means) of protecting personal information.[234]

Hashing is a process of translating personal data into corresponding (but shorter) strings of randomised characters, and permits a data matching partner to receive data from different sources and match it without directly viewing the personal information underneath.[235] For example, a third party advertiser can match the cookie of a user who has provided her email address to a partner website, with the mobile activities (via an advertising ID) of a user who has provided that same email address to any partner app. Although such actions may ostensibly be taken to avoid restrictions that partners may have around sharing personal information,[236] hashed (pseudonymised) data remains personal information.[237]

(l) Encrypted data

Data can be securely communicated over the internet in plain text or via the HTTPS protocol[238] using Transport Layer Security (TLS), which replaces Secure Socket Layer (SSL),[239] to authenticate and encrypt the connection. In relation to mobile applications, an online service (the app developer's website) must present a TSL or SSL certificate[240] to the

---

[233] GDPR art 4(5) defines the term as 'the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person'. The term is not defined elsewhere, but the practice is clearly one which can be adopted by app developers in those jurisdictions.

[234] Ibid rec 26, 28, 29, 75, 85 and 156.

[235] Future of Privacy Forum, *Cross Device: Understanding the State of State Management* (November 2015) at 8.

[236] Ibid.

[237] See the detailed discussion of the concept of 'personal information' in chapters 4, 5 and 6.

[238] Hypertext Transfer Protocol Secure (HTTPS). Although the data is encrypted there are still risks that hackers can intercept and decrypt communications. Wikipedia, 'HTTPS' <https://en.wikipedia.org/wiki/HTTPS#cite_note-6> accessed 27 February 2020.

[239] For the use of credit card payments, the transition deadline to TLS v1.1 or higher under the Payment Card Industry Data Security Standard (PCI DSS) v3.2 was 30 June 2018. See Payment Card Industry (PCI) Security Standards Council, 'Migrating from SSL and Early TLS: A Resource Guide from the PCI Security Standards Council' (2018) <https://www.pcisecuritystandards.org/pdfs/PCI_SSC_Migrating_from_SSL_and_Early_TLS_Resource_Guide.pdf?agreement=true&time=1582791832037> accessed 27 February 2020. E.g., PayPal supports only merchants running TLS v1.2.

[240] This is an electronic certificate issued by a trusted third party, an approved Certification Authority (CA), to a domain hosted on the World Wide Web. The certificate will authenticate and encrypt communications with

app on the user's device. The app must validate the certificate and will then permit communication from the app to the app developer's servers.

The OS platform plays a key role in security by making security APIs available to developers that will block connections if an invalid SSL/TSL certificate is presented to the app. [241] It is the responsibility of developers to use these tools to minimise the risk of a data breach such as a man-in-the-middle attack. [242] Tools to test for SSL/TSL certificate validation vulnerabilities are also publicly available to developers at little or no cost.[243] To enhance security further, developers can 'pin' their certificate to their mobile app to ensure that the app will not communicate with any other server.[244] For the app user, there are as yet no standardised means of verifying that the communication is secured, even if the app's marketing, privacy policy and terms and conditions state that it is.[245] The review policy of app platforms is thus crucial. Google recently announced that 80% of Android apps now have

servers at this domain using public-private key encryption. A certificate can be issued only in accordance with International Telecommunications Union Standardisation Sector (ITU-T), *X.509 : Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks* (October 2016). There are a number of commercial CAs (including Symantec, Comodo and GoDaddy) and their resellers who offer SSL and TSL certificates. Wikipedia, 'Certificate Authority' <https://en.wikipedia.org/wiki/Certificate_authority> accessed 27 February 2020.

[241] OS Platforms are introducing stronger encryption protocols for new OS versions. E.g. Android 8.0 Oreo no longer supports SSL v3 but earlier versions do. Android Developers, 'Android 8.0 Behavior Changes' <https://developer.android.com/about/versions/oreo/android-8.0-changes> accessed 19 February 2020. From 1 November 2019, all new Android apps must target Android 9 (Pie) with TLS encryption enabled by default. Apple by default enables TLS v1.2 through its App Transport Security (ATS) for apps linked to iOS v9.0 or higher. Apple Developer Centre, 'Preventing Insecure Network Connections' <https://developer.apple.com/documentation/security/preventing_insecure_network_connections> accessed 27 February 2020 and Apple Developer Centre, 'Security' <https://developer.apple.com/security/> accessed 27 February 2020. Both OS by default limit communication to certificates from CAs trusted by the OS. However, in both OSs, customisation of the code makes it possible for developers to permit insecure (HTTP) connections to particular servers, to user-trusted certificates and for certain activities such as web views or media downloads.

[242] *In the Matter of Fandango LLC* FTC Dkt No C-4481 (24 August 2014) (consent order), complaint at para 10–14. A man-in-the-middle attacker situates itself between the consumer's device and the online service by presenting an invalid SSL certificate for the application.

[243] Ibid.

[244] Doug Dooley, 'Putting TLS Pinning in Your Mobile Apps' (*Infosecurity Magazine*, 26 October 2018) <https://www.infosecurity-magazine.com/opinions/tls-pinning-mobile-apps/> accessed 27 February 2020.

[245] In a web-context the website the user is visiting will display the SSL certificate seal and the https protocol in the URL. Browsers store 'trusted' certificates and will display a warning if an invalid certificate is displayed. Browsers are configured slightly differently but use e.g. green-coloured text in the URL or a lock symbol to alert users that the communication is secure.

default encryption,[246] but if apps that do not have encryption are not taken down from app stores, they will continue to pose a risk to users.

The FTC investigation into the Fandango movies app[247] illustrates the need for app developers to correctly implement encryption techniques[248] and use a secure payment service provider.[249] Fandango's free movies app allowed users to purchase movie tickets 'on the go'. After making a purchase, the user would be presented with payment options, including credit card.[250] The credit card number entered by the user (or previously saved on the device), CVV security code, expiration date and billing zip code would be transmitted to Fandango's servers. Users had a choice whether to create an account in the app, and if they logged into the app using their account details, their authentication credentials (email address and password) would also be transmitted.

Fandango's in-app privacy statement represented to users reads as follows:

> *'Your Fandango iPhone Application allows you to store your credit card and Fandango account information on your device so you can conveniently purchase movie tickets. Your information is securely stored on your device and transferred with your approval during each transaction.'*[251] *(Own emphasis.)*

In fact, Fandango had bypassed the default settings provided by the iOS APIs and had failed to implement any other certificate validation measures. Its app testing and security audits were inadequate because they had not considered the risk of certificate validation vulnerabilities. Furthermore, there was no system to receive security reports. A customer reported the vulnerability to Fandango, but the app's customer service portal tagged

---

[246] C Scott Brown, '80% of Android apps are encrypting traffic by default, up from 0% in early 2018' (*StackExchange*, 3 December 2019) <https://www.androidauthority.com/android-app-encryption-1062202/> accessed 27 February 2020.

[247] *In the Matter of Fandango LLC*.

[248] Also see Android Developers, 'Security with HTTPS and SSL' (27 December 2019) <https://developer.android.com/training/articles/security-ssl> accessed 27 February 2020.

[249] E.g., give users an option to pay with their PayPal account. To do this a developer would integrate the PayPal mobile payments library into the app code. When a user selects 'pay with PayPal' the library would initialise a PayPal 'checkout experience'. The transmission of payment data would thus be handled by PayPal and not by the developer. See PayPal Developer, 'Get started with mobile payment libraries' (2020) <https://developer.paypal.com/docs/archive/mobile/gs_MPL/> accessed 27 February 2020.

[250] Collection of credit card information requires compliance with Payment Card Industy (PCI) Security Standards Council, *PCI Data Security Standard v3.2* (2016). From 30 June 2018 this requires the app to have a TLS certificate.

[251] The statement is somewhat ambiguous as to whether both on device storage and transfer are 'secure', but Fandango also represented on the purchase page 'You don't need an account to *securely* purchase tickets.'

the communication as a password reset and flagged it as resolved. It thus never received attention from Fandango.[252]

(m) Data mining

Data mining involves the analysis of 'big data'. This further processing may be unrelated to the immediate purpose of collecting and processing data, and it will usually combine the data with data from other sources.[253] It may involve sharing the data with third parties (whose identity and purpose in acquiring the data are again unknown to the data subject).[254] Not only will the further processing not be disclosed to the data subject, but the purpose of processing is usually unknown (and thus cannot be disclosed at the time of data collection) since analytics seeks to make predictions or derive new insights, rather than to answer pre-determined questions.[255]

(n) Data Leaks and Data Breaches

A data breach involves hackers exploiting weak security measures to obtain access to a network and the personal information stored or transmitted within that network.[256] Recent scandals involving Liberty,[257] Facebook,[258] Equifax[259] and Uber[260] have drawn public

---

[252] The FTC viewed Fandango's disclosures to users as deceptive as it actual security practices were not secure. In terms of the consent order, Fandango was required to implement a comprehensive security program and submit to independent biennial audits for 20 years. The FTC is empowered under s 5 of the Federal Trade Commission Act of 1914, 15 U.S.C. §§ 41–58 (2018) (FTCA)to investigate unfair and deceptive trade practices.
[253] Bruening and Culnan at 562.
[254] Ibid.
[255] Ibid.
[256] GDPR art 4(12) defines a 'personal data breach' as 'a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.'
[257] Tehillah Nieselow, 'Five Massive Data Breaches Affecting South Africans' *Mail & Guardian* (19 June 2018) <https://mg.co.za/article/2018-06-19-five-massive-data-breaches-affecting-south-africans/> accessed 8 March 2020.
[258] Mike Isaac and Sheera Frenkel, 'Facebook Security Breach Exposes Accounts of 50 Million Users' *NY Times* (28 September 2018) <https://www.nytimes.com/2018/09/28/technology/facebook-hack-data-breach.html> accessed 8 March 2020.
[259] See e.g. *In re Equifax Inc. customer data security breach litigation* 362 F Supp 3d 1295 (ND Ga 2019) where failure to implement a software security patch permitted hackers to access sensitive personal information of 147 million US consumers held by the credit bureau Equifax, including names, addresses, birth dates, social security numbers, driver's license information, telephone numbers, email addresses, tax identification numbers, credit card numbers, and credit report dispute documents. A $600 million settlement has been approved by the courts, but an appeal by objectors is pending. 'Equifax Data Breach Settlement' <https://www.equifaxbreachsettlement.com/> accessed 26 February 2020.
[260] Following discovery of a payment of $100 000 by Uber to hackers to cover up evidence of a data breach involving millions of Uber customers and drivers names, email addresses and telephone numbers (stored in a third-party cloud storage service) Uber has been ordered to pay a $148 million penalty, and submit to external

attention to the potential privacy impact for consumers, although statutory definitions[261] and breach notification requirements differ.[262]

Although the terms are sometimes used interchangeably,[263] the term 'data leak' is used here to refer to personal information that is exposed without any actor penetrating the system or subverting platform rules. For example, Cambridge Analytica's use of Facebook profiles and likes of app users and their friends to infer political leanings[264] and ad network InMobi Pte's use of Wi-Fi connectivity data to infer user location[265] 'leaked' personal information to third parties but could not be classified as a security breach.[266]

(o) Personalisation

When apps disclose that they collect personal information to 'customise' or 'personalise' the app, this could cover a number of activities from personalised greetings in communications

---

audits of its implementation of model security breach notification and security protocols. New York Attorney General, 'A.G. Underwood Announces Record $148 Million Settlement With Uber Over 2016 Data Breach ' (26 September 2018) <https://ag.ny.gov/press-release/2018/ag-underwood-announces-record-148-million-settlement-uber-over-2016-data-breach> accessed 2 March 2020. Uber agreed in 2016 to implement measures to encrypt and restrict employee access to geolocation and other sensitive data. New York Attorney General, 'A.G. Schneiderman Announces Settlement with Uber to Enhance Rider Privacy' (6 January 2016) <https://ag.ny.gov/press-release/2016/ag-schneiderman-announces-settlement-uber-enhance-rider-privacy> accessed 2 March 2020.

[261] POPIA uses the term 'security compromises' in s 22(1): 'Where there are reasonable grounds to believe that the personal information of a data subject has been accessed or acquired by any unauthorised person, the responsible party must notify–
(a) the Regulator; and
(b) subject to subsection (3), the data subject,
unless the identity of such data subject cannot be established.'
Section 21(2) requires an operator to notify the responsible party as soon as it becomes aware of a security compromise.

[262] Both GDPR and POPIA contain breach notification requirements. In the US there is no federal breach notification requirement under the COPPA Rule 16 C.F.R §312. Uber was prosecuted under state laws, and breach notification to the US Department of Health and Human Services is a requirement under Health Insurance Portability and Accountability Act of 1996, Pub.L. No. 104–191, 110 Stat. 1936 (HIPAA). See generally Federal Trade Commission, *Data Breach Response: A Guide for Business* (May 2019). An analysis of the data breach notification requirements, falls outside the scope of this dissertation.

[263] In media and industry news there is general confusion about whether the terms are distinct, which may be attributed to the lack of common statutory definitions, and the absence of judicial and regulatory interpretative guidance. This is an important area for future legal study given the ramifications for failing to comply with statutory breach notification requirements.

[264] Hern op cit note 119.

[265] See *United States v InMobi Pte Ltd*. For a recent technical explanation in relation to current Android permission settings see Verga and others.

[266] It is beyond the scope of this dissertation to consider the myriad security risks and their guises.

to saving user preferences, assigning a custom 'avatar',[267] and speeding up check-outs on e-commerce apps by saving shipping and payment information. It could provide convenient utilities, such as an app that provides you with an updated weather forecast at your location. However, it also means recommending content, products, services, contacts ('friends') and events (either in-app, or by push notifications or email) based on personal information.[268] This element of customisation is popular with users and results in greater user 'engagement'.[269]

Personalisation is thus an important success strategy for app developers.[270] For example, Spotify uses listener data to customise playlist suggestions and send users in-app notifications and emails about new releases and local concerts or shows they might be interested in.[271] Similarly, Netflix recommends movies based on viewing history, Amazon recommends products based on purchase history and product likes, Instagram helps users 'discover' content relevant to their interests and those they follow, and Facebook provides reminders about birthdays, and 'friendiversaries', and personalises the users' newsfeed with content based on their interests.[272] However, these types of 'personalisation' are in fact 'profiling', for which the user should give opt-in consent after being informed about what information is collected, how it is used and with whom it is shared.

(p) Profiling and information matching

Profiling refers to automated processing of personal information to evaluate the characteristics of a user, make predictions about their behaviour and target them with, for example, interest-based advertising.[273] However, profiling can also be a feature of so-called 'personalised apps' which recommend content, products and local events (both in the app and via push

---

[267] In the virtual world an avatar is a graphical representation of an individual, either as a 3D character (e.g. in online games) or as a 2D icon. Techopedia, 'What is an avatar?' <https://www.techopedia.com/definition/4624/avatar> accessed 13 April 2020.
[268] Taplytics, 'App Personalization: The 5 Best Personalized Apps' (28 March 2019) <https://taplytics.com/blog/app-personalization-5-best-personalized-apps/> accessed 4 March 2020.
[269] In short, they use the app more often, and for longer periods.
[270] Taplytics.
[271] Ibid.
[272] Ibid.
[273] GDPR art 4(4) defines 'profiling' as 'any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.' Although the term is not defined in POPIA it is used in the same sense in s 71 (discussed further in chapter 6). COPPA Rule 16 C.F.R §312.2 and CCPA §1798.140 do not define profiling, but expressly exclude it from the scope of processing for 'internal support'/'business purposes' for which there are more relaxed notice and consent requirements as discussed in chapter 4.

notifications and email) based on user interests. As such, profiling is somewhat different from information-matching programs, which imply comparison of different records, each containing reference to multiple data subjects.[274]

(q) Nudging

Nudges are '"soft paternalistic" behavioural interventions that do not restrict choice but attempt to account for decision-making hurdles'.[275] While nudges can be used for corporate-profit enhancement, they also carry potential benefits for users – for example, Discovery Vitality's 'rewards' for healthy lifestyle choices. Nudges can also be used to overcome the complexities facing users in managing their online privacy. OS and social media platforms can play an important role in this regard. For example, Facebook's "Privacy Check-up" interrupts users when making public posts to inform them about options for limiting who can view posts and directing them to additional privacy information.[276] However, app developers can also utilise the concept of privacy nudges to develop 'privacy-friendly' apps.[277]

VII PERSONAL INFORMATION COLLECTED BY MOBILE APPS

When an app requires a user to create a profile, the user may volunteer a range of personal information such as name, birthdate, email address and password. The account name,[278] email address, unique device identifier[279] or device fingerprint[280] can be collected. On an OSN, user profiles can include a range of other personal information such as address, education,

---

[274] POPIA s 1 defines an 'information matching program' as 'the comparison … of any document that contains personal information about ten or more data subjects with one or more documents that contain personal information of ten or more data subjects, for the purpose of producing or verifying information that may be used for the purpose of taking any action in regard to an identifiable data subject.'

[275] Hazim Almuhimedi, 'Helping Smartphone Users Manage their Privacy through Nudges' (DPhil, Carnegie Mellon 2017) at 1.

[276] Ibid at 2. Permission settings in the OS can operate as a privacy nudge. E.g. by alerting users to an app request to access background location.

[277] Bin Liu, 'Can Machine Learning Help People Configure Their Mobile App Privacy Settings?' (DPhil Carnegie Mellon 2019).

[278] E.g. an Apple ID created by the user of Apple devices and G-Suite account name by Google users.

[279] Examples discussed above include device serial number (IMEI or MEID), MAC address, Apple device serial number, Apple UDID, and Android ID and Android OsBuild code assigned to Android devices. Android 8.0 Oreo has introduced a new privacy feature which displays a different Android ID to apps with different signing keys (i.e. even when those apps are running on the same device, each of them will have a different Android ID for that user). Android Developers, 'Android 8.0 Behavior Changes'. This does not prevent a developer using the same signing key for multiple apps (and then being able to link the Android ID to multiple apps) but it would restrict some of the downstream aggregation of personal information linked to Android IDs.

[280] gdad-s-river, 'Metadata: Story Of How Whatsapp And Other Chat Apps Collect Data' (*Fossbytes*, 27 January 2017) <https://fossbytes.com/whatsapp-chats-collect-data-metadata/> accessed 26 October 2019.

employment, relationship status, family and interests.[281] In addition, users may upload photos and videos and reveal their opinions, activities and interests through posts, likes, shares, tags, sending and accepting friend requests, joining groups and using applications.[282]

The user has some control through privacy settings over the extent to which this information is visible to other users. These settings are determined by the OSN provider, not by the developer of any app that connects to the OSN. For example, Liu discusses the development of 'privacy friendly' settings by Facebook, which changed the default setting from 'public' to 'friends only' in 2014, and permits additional granular control in custom privacy settings.[283] But (despite privacy settings) the information is still transmitted to the OSN provider and the user has limited knowledge and no direct control over whether it is shared by the OSN with third parties such as ad networks.[284] Unlike applications running through web browsers, mobile apps can access unique mobile device identifiers, contacts, calendar entries, SMS, phone calls, email, and documents, photos and videos in device storage. [285] The app can also access data from on-device sensors[286] such as GPS,[287] camera, microphone,[288] accelerometer,[289] magnetometer,[290] gyroscope,[291] biometric sensors,[292] and many more.[293] Thirdly, although apps are 'sandboxed' to prevent interference with the functioning of the device and other apps on the device, it is possible for apps to share data with other apps.

---

[281] Liu at 8.
[282] Ibid.
[283] Ibid, at 9. Also at 28–33 on the limitations of user privacy settings in Facebook, for example.
[284] Ibid at 3.
[285] Various authors provide similar lists of the types of information accessible to apps. See ibid.
[286] These will differ according to device and version.
[287] Through satellite communication a Global Positioning System (GPS) unit can provide a precise location. Apps can request permission for this 'fine-grained' location, e.g. Uber and Google Maps. Apps can also request permission for 'coarse-grained' location, which would place the user in a particular area, such as a city, but would not provide an exact location.
[288] Which in the case of digital assistants such as Siri and Alexa would 'listen in' at all times to detect voice commands and search requests.
[289] For acceleration, vibration and tilt. An app can use this to tell if the phone is in portrait or landscape mode and adjust the display. Apps can also use this to tell the speed at which a user is walking/running/driving.
[290] Compass.
[291] Measures the degree and angle of rotation. It is used in apps that need to understand precisely where the phone is pointing, such as Pokémon Go and astronomy apps.
[292] Such as fingerprint and face recognition.
[293] For a complete list see Manisha Priyadarshini, 'Which Sensors Do I Have In My Smartphone? How Do They Work?' (25 Sept 2018) <https://fossbytes.com/which-smartphone-sensors-how-work/> accessed 29 October 2019.

Access by the app to data on the device or in other apps is controlled through 'permissions' determined in the API of the OS. However, weaknesses in the permission architecture, and user apathy or ignorance, mean that apps can access such information without a user's full knowledge and understanding. Furthermore, malicious applications can exploit security vulnerabilities in the OS architecture to bypass permission settings.

It must be reiterated that as there is little quantifiable data about what personal information apps collect,[294] this section describes what it is possible for an app to collect, but does not indicate what personal information is actually being collected, or that the collection of this information triggers legal responsibility under data protection laws.

VIII ONLINE ADVERTISING: GENERIC, CONTEXTUAL AND TARGETED ADVERTISEMENTS

Online ads can be broadly characterised as generic, contextual or targeted.[295] At one time, mobile apps primarily served generic ads, leading to low 'click through rates' and consequently low revenue.[296] Contextual ads are displayed based upon relevance to the content being viewed.[297] In the online web-based context, Google AdSense pioneered the use of bots to crawl and index web pages so that ads could be delivered that are relevant to the content on the webpage.[298] In a mobile applications context, a different approach is required, and contextual ads are matched to the relevant app category.[299] In this sense, the ad is targeted at a particular audience, but not at a particular user, and no personal information about the user is retained.[300]

---

[294] The limited number of studies on the subject do not always refer to 'personal information' or align their use of the concept with the legal definition. Furthermore, Liu's study outlines the difficulty of isolating which traffic (data flows) contain PI. He defines 'personal information' somewhat ambiguously at 5, as 'information about user's demographics or other identifiable information, including personally identifiable information (PII), but not necessarily lead (sic) to distinguish or trace an individual identity'. This suggests a gap in knowledge of how to apply the legal concept of 'personal information' in the context of app development and data processing.

[295] Imdad Ullah and others, 'Characterising User Targeting for In-App Mobile Ads' in *2014 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)* (IEEE, Toronto, ON, 22 April - 2 May 2014).

[296] Suman Nath and others, 'Smart Ads: Bringing Contextual Ads to Mobile Apps' in *Proceeding of the 11th Annual International Conference on Mobile Systems, Applications, and Services* (ACM, Taipei, Taiwan 25–28 June 2013).

[297] Ibid.

[298] Ibid.

[299] Ullah and others (2014).

[300] Contextual advertising is defined by the US Federal Trade Commission as 'the delivery of advertisements based upon a consumer's current visit to a Web page or a single search query, without the collection and retention

Ullah defines a targeted ad as one delivered to a particular user based upon their user profile, comprising interests, age, gender, or other characteristics of a selected user.[301] This broad categorisation should be distinguished from location-based advertising, which serves ads specific to the user's current location.[302] Profiling user interests, which may include app behaviour (for example, a heavy gamer)[303] or ad behaviour (ads viewed or clicked on previously) permits *behaviourally* targeted ads.[304] Re-targeting (or re-marketing) is the practice of delivering ads based on activity to users on a website or in an app when they visit other websites.[305] As an example, the owner of a YouTube channel can 'remarket' its product to viewers of its channel by delivering ads for its products to the same user when they visit another website. This is enabled by tracking a persistent identifier assigned to that user, such as an advertising ID.[306]

Targeted advertising is highly effective[307] and in theory benefits all parties,[308] including the app user for whom receipt of personally relevant adverts may be desirable.[309] For example, a 2012 national poll of over 700 regular internet users in the US showed that 84% preferred targeted advertising in exchange for free online content.[310]

---

of data about the consumer's online activities over time.' Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for businesses and policymakers* (March 2012).

[301] Ullah and others at 548. Ullah (2017) at 1 lists device attributes (e.g. OS version, device type/version, browser type/version, connectivity type, mobile operator etc.), user's temporal behaviour, demographics, interests, apps categories, and locations. To this may be added the Android advertising ID. There is some scope of overlap in characterisation, and a considerable lack of transparency by ecosystem role-players. E.g. successful mobile ad network Tapjoy describes the targeting criteria for contextual advertising as 'including app category, target demographics [age, gender], and a variety of user-specific data points available to advertisers'.

[302] Paul E Ketelaar and others, '"Opening" Location-Based Mobile Ads: How Openness and Location Congruency of Location-Based Ads Weaken Negative Effects of Intrusiveness on Brand Choice' (2018) 91 *Journal of Business Research* 277–285.

[303] Ullah and others at 547.

[304] Google refers to this as personalised (interest-based) ads.

[305] Liz Feller, 'Mobile App Retargeting: Benefits and Best Practices' (*Branch*, 22 March 2019) <https://blog.branch.io/mobile-app-retargeting-benefits-and-best-practices/> accessed 5 March 2020.

[306] *United States of America and People of the State of New York v Google LLC and YouTube LLC* Case No 1:19-cv-02642 (DDC Sep 10, 2019) (draft consent order).

[307] Ullah at 1.

[308] Ibid.

[309] Ibid at 9.

[310] Annalect Group, *Internet Users' Response to Consumer Online Privacy* (2012) at 7. This statistic is quoted by J.T. Rosch, *Dissenting Statement of Commissioner J. Thomas Rosch: Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers* (March 26, 2012) [citing a media report of the survey by Katy Buchman, 'Study: Internet User Adoption of DNT Hard to Predict' (20 March 2012) <https://www.adweek.com/digital/study-internet-user-adoption-dnt-hard-predict-139091/> accessed 4 March 2020].

However, targeted advertising also raises grave privacy concerns related to the profiling and tracking of users that may outweigh its perceived benefit to users.[311] A 2018 report indicates that through real time bidding on ad exchanges, advertisers receive a large amount of personal information about users.[312] The information shared included 'the URL of every page a user is visiting, their IP address (from which geographical position may be inferred), details of their device, and various unique IDs that may have been stored about the user previously to help build up a long term profile about him or her'.[313] This data is linked to a 'data broker segment ID' based on 'income bracket, age and gender, habits, social media influence, ethnicity, sexual orientation, religion, political leaning, etc.'.[314]

The ability to profile users is facilitated in the mobile environment by three key differences between in-app and web-based advertising.[315] First, the permissions granted by the user to the application are automatically accessible to the ad library.[316] Secondly, smartphones permit access to highly sensitive data, including call logs, location and camera, and permissions can allow apps (and hence ad libraries) to read and write calendar entries, and send phone calls and text messages.[317] Thirdly, mobile devices have persistent or quasi-

---

[311] The Annalect Group survey reveals somewhat conflicted user responses as all respondents viewed privacy as important and 83% said they would use a 'Do Not Track' mechanism. The trade-off that consumers appear unwilling to make is to pay for presently free content. Also see Ullah at 6.

[312] Johnny Ryan, 'Report from Dr Johnny Ryan – Behavioural advertising and personal data' (5 September 2018) <https://brave.com/wp-content/uploads/Behavioural-advertising-and-personal-data.pdf> accessed 26 February 2020. An investigation opened in May 2019 by the Data Protection Commission Ireland (lead supervisory authority over Google in Europe) is ongoing, following complaints to data regulators across Europe about the operation of ad exchanges. Data Protection Commission Ireland, 'Data Protection Commission opens statutory inquiry into Google Ireland Limited' (22 May 2019) <https://www.dataprotection.ie/en/news-media/press-releases/data-protection-commission-opens-statutory-inquiry-google-ireland-limited> accessed 26 February 2020. The press-release records that the investigation will consider GDPR compliance of each stage of processing (with, inter alia, the principles of transparency and data minimisation) and Google's data retention practices. A further investigation was opened on 4 February 2020 into Google's Data Protection Commission Ireland, 'Data Protection Commission launches Statutory Inquiry into Google's processing of location data and transparency surrounding that processing' (4 February 2020) <https://www.dataprotection.ie/en/data-protection-commission-launches-statutory-inquiry-googles-processing-location-data-and> accessed 26 February 2020.

[313] Ryan at 2.

[314] Ibid at 4.

[315] Stevens and others at 2.

[316] Ibid. Although, subsequent to this publication, with the introduction of Android 6.0 (Marshmallow), dangerous permissions can be requested only at runtime (and users can revoke or vary permissions in settings), this does not address the failure to distinguish between app (first party) and third party permissions. See: Binns and others.

[317] Stevens and others at 3. The study by Stevens found that several ad networks were accessing sensitive permissions even when this was not disclosed in the ad library's documentation.

persistent identifiers that can be used to track an individual across apps and across platforms.[318]

In a traditional web-browser, the IP address and cookies are not persistent, and can be reset, blocked or masked by the user.[319] Additionally, there are a greater number of user controls and choices available of browsers[320] and in-browser settings, such as the browser tool by the Digital Advertising Alliance (DAA), which checks for first-party and third-party cookies, and Google's advertising links.[321]

In the Android mobile environment, advertisers are now permitted to access only the Android Advertising ID (AAID),[322] which is a unique identifier that can be reset by the user, and permits users to opt out of personalised ads.[323] Apple has an ID for Advertisers (IDFA) which replaces use of the unique device identifier (UDID) for ad tracking.[324] Developers must access the Advertising ID only through the Advertising ID API and must have a link to a valid privacy policy accessible within the appropriate field of the Play Console and in the app that notifies users of the collection and user of the Advertising ID.[325] In terms of its developer contract, Google can remove apps from the app store that do not comply with this policy. The release of iOS 12 and Android P in 2018 app platforms introduced tightened security measures for apps, and app stores have also tightened up on their review process.

---

[318] Ibid. Note the subsequent changes in Google policy discussed below partly address this issue.

[319] An IP address changes periodically. Cookies, even if they are persistent cookies, can be deleted or blocked altogether by the user in browser settings. Using a browser such as TOR allows a user to mask their identity altogether.

[320] Mozilla Firefox for example takes steps to limit ad tracking.

[321] Google displays ads in the browser with a link which users can follow to an explanation of why they are seeing the ad, where their information was obtained, and how they can control ad settings. Google LLC., 'How Google shows you ads' <adssettings.google.com> accessed 3 November 2019.

[322] Android Developers, 'Best Practices for Unique Identifiers' <https://developer.android.com/training/articles/user-data-ids> accessed 26 February 2020. Apple introduced similar changes on its developer platform in 2013.

[323] If the Advertising ID is never (or infrequently) reset it will, however, act as a quasi-identifier of the individual, or their device. Under the device settings, by selecting services and ads, users can turn on the "opt out" button. Google Play Console Help, 'Advertising ID' <https://support.google.com/googleplay/android-developer/answer/6048248?hl=en> accessed 24 October 2019. Both methods rely on user action to override default settings that permit a degree of tracking.

[324] Allison Schiff, 'Mobile Device IDs Will Be The Next Ad Tracker To Bite The Dust' (10 February 2020) <https://www.adexchanger.com/mobile/mobile-device-ids-will-be-the-next-ad-tracker-to-bite-the-dust/> accessed 22 April 2020. Changes are occurring quickly in the ecosystem, and the use of advertising identifiers may be phased out. However, tracking is difficult to police. As indicated under 'device fingerprinting', other device features (and even the user's cellular phone number) can be collected to identify a device uniquely.

[325] Google Play Developer Policy Centre, 'Advertising ID ' <https://play.google.com/about/monetization-ads/ads/#!?zippy_activeEl=ad-id#ad-id> accessed 24 October 2019. The policy must be adhered to in terms of s 4.1 of the Google.

Both Google Play and Apple now require apps to have a privacy policy. Anecdotally, app developers continue to suggest a 'quick fix'[326] relying on free online privacy policy generator tools.[327] Users can opt out of interest-based advertising (but will still receive in-app ads),[328] and can disable 'push notifications' or block notifications to the device's 'lock screen', using system settings.[329]

Other persistent device identifiers remain accessible for 'specific use cases' provided they are not advertising related.[330] These persistent unique identifiers were described by Stevens as:[331]

1. The Android device ID (SSAID), generated during the first boot of a device, which can be deleted only with a factory reset.[332]
2. The smartphone's device ID.[333]
3. The android.os.Build.code, which is not wiped on a factory reset.[334]
4. The MAC address utilised for Wi-Fi and Bluetooth services.[335]

The privacy risks are both direct and indirect. First, there is the information made available directly to advertising networks and analytics companies, which may include personal information. Secondly, there is the possibility that ad and analytics companies aggregate data from multiple third party trackers[336] and can infer personal information such

---

[326] S Swaroop, 'How to fix Advertising ID policy violation in Google Play Store really quick?' (25 September 2018) <https://blog.usejournal.com/how-to-fix-advertising-id-policy-violation-in-google-play-store-6d9cf92d335d> accessed 24 October 2019.
[327] E.g. 'App Privacy Policy Generator' <https://app-privacy-policy-generator.firebaseapp.com/> accessed 16 May 2019.
[328] Google Play Developer Policy Centre, 'Advertising ID '.
[329] Android Developers, 'Notifications Overview'.
[330] Google states: 'You can use persistent identifiers as long as you have a privacy policy and handle the data in accordance with the Developer Distribution Agreement and all applicable privacy laws in the areas where you make your app available.'
[331] Stevens and others.
[332] This is distinguishable from the ANDROID Advertising ID which is resettable by a user in browser settings. IPhones have a Universal Device ID (UDID).
[333] Stevens and others. This is the International Mobile Equipment Identity (IMEI) number for GSM phones. Global System for Mobile Communications (GSM) is a standard developed by the European Telecommunications Standards Institute (ETSI). It is the mobile equipment identifier (MEID) or Electronic Serial Number (ESN) for the CDMA technical standard developed by the 3rd Generation Partnership Project 2 (3GPP2). In the Apple eco-system, this includes the Apple serial number of the device.
[334] Ibid.
[335] Ibid. The MAC address is the media access control (MAC) number assigned to a network interface device (i.e. a device that can connect to another networked device via Ethernet cable, Wi-Fi or Bluetooth).
[336] Ullah at 2.

as shopping habits, socio-economic class or even political opinions from the data collected,[337] or in combination with data gleaned from social networks.

Indirectly, 'privacy leaks' may make personal information available to other unknown and possibly malicious third parties. For example, the delivery of ads to apps via unencrypted traffic may enable third parties to infer interests (if they know that targeted advertising is taking place). Furthermore, the spoofing of a device ID[338] permits the interception of communications. Tracking of the MAC address,[339] and exploitation of Bluetooth connections,[340] also permit access to personal information.

However, the ability to collect such information does not automatically mean it is being shared with third parties. Nor does the sharing of data within the advertising industry mean that personal information is being sold. Publishers and advertisers may be given aggregated statistics showing particular segments or audiences. There is as yet no standardisation in relation to how aggregation is achieved, and at what point data becomes anonymised, and various approaches to privacy and security may be applied. The measures to secure privacy are technologically advanced and complex, and cannot be implemented within the app by developers. They must be implemented by ad networks and ad exchanges.

---

[337] Binns and others.

[338] 'Spoofing' refers to hackers impersonating a device by using its device ID. Researchers have demonstrated that device spoofing could enable personal data to be obtained from mobile analytics services. Terence Chen and others, 'Information Leakage Through Mobile Analytics Services' in *HotMobile '14: Proceedings of the 15th Workshop on Mobile Computing Systems and Applications* (ACM, Santa Barbara CA 26–27 February 2014). Failure to correctly employ encryption techniques renders data transmitted by an app through a public Wi-Fi network exposed to 'man-in-the middle' attacks where hackers use an invalid SSL or TLS encryption certificate to intercept communications between a user's device and a mobile app server. See *In the Matter of Fandango LLC* and the discussion of encryption below.

[339] Smartphones with Wi-Fi enabled will continuously search for available Wi-Fi networks by broadcasting the device MAC address. This can be used to track users in public Wi-Fi 'hotspots', sometimes by hackers but also by businesses and governments. E.g. the London underground tracked tube users to determine how to improve congestion and where advertising was best placed. Gareth Corfield, 'TfL to track Tube users in stations by their MAC addresses' (27 November 2016) <https://www.theregister.co.uk/2016/11/17/tfl_to_track_tube_users_by_wifi_device_mac_address/> accessed 26 February 2020. The technique of MAC randomisation (where the device substitutes a randomly generated number) is neither standardised nor uniformly implemented across devices, and remains open to re-identification attacks. Jeremy Martin and others, 'A Study of MAC Address Randomization in Mobile Devices and When It Fails' in *Proceedings on Privacy Enhancing Technologies* (De Gruyter Open, Minneapolis, USA 18–21 July 2017).

[340] Recent work has exposed the leak of personal information from Apple's Bluetooth-enabled device continuity – the ability to sync multiple devices via Bluetooth. Jeremy Martin and others, 'Handoff All Your Privacy: A Review of Apple's Bluetooth Low Energy Implementation' [2019] <arXiv preprint arXiv:1904.10600> accessed 15 May 2020, and Guillaume Celosia and Mathieu Cunche, 'Discontinued Privacy: Personal Data Leaks in Apple Bluetooth-Low-Energy Continuity Protocols' (2020) 1 *Proceedings on Privacy Enhancing Technologies* 26–46.

Some approaches that appear promising are differential privacy techniques to add 'noise' to data, such as k-anonymity, l-diversity and t-closeness,[341] and cryptographic methods to retrieve relevant ads securely from an advertising database server without revealing private information to advertising networks[342]

IX THE MOBILE "CLOUD"

Cloud computing, which is relatively new, having developed since about 2007, harnesses the networking capabilities of the internet to provide users with access on demand to computing resources on a pay-per-use basis (an operating expense) without the need for costly upfront purchases of hardware and software (a capital expense). As mobile devices are lightweight terminals with limited storage and processing capacity, the transition to mobile has accelerated the adoption of cloud services. The result is 'a generation of consumers/end-users who accept the "cloud" environment as the normal way to access information, services and communications'.[343]

Cloud computing has been defined as

> '*a model for enabling ubiquitous, convenient on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction*'.[344]

It is not a specific technology and is better 'understood as a service model for computing services based on a set of computing resources that can be accessed in a flexible, elastic, on-demand way with low management effort'.[345]

---

[341] Ullah at 23.
[342] Ibid.
[343] Adrian Schofield, *Research Study on the Economic Impact of Cloud Services on South African SMMEs* (Johannesburg, Johannesburg Centre for Software Engineering: University of Witwatersrand, 2013) at 16.
[344] US National Institute of Standards and Technologies (NIST).
[345] OECD Directorate for Science, Technology & Industry Committee on Digital Economy Policy 'Cloud computing: The concept, impacts and the role of government policy' (19 Aug 2014) at 8. Available at http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DSTI/ICCP(2011)19/FINAL&docLanguage=En, accessed on 27 February 2018.

Clouds can be public, private, community or hybrid clouds.[346] Three main cloud service models have been identified:

- Infrastructure as a Service (IaaS): provides raw computing resources, allowing the user maximum flexibility to run its own operating systems and software.
- Platform as a Service (PaaS): provides a structured platform on which users can run their own application or service through a dedicated API (raising issues of lock-in to a particular cloud service provider).
- Software as a Service (SaaS): the user directly accesses applications of the cloud provider. Examples are e-mail, CRM, document management and accounting software.[347]

The term 'mobile cloud computing' covers any use of cloud services on mobile devices. It is what makes it possible for resource- and data-intensive mobile applications to run seamlessly on a device that has limited storage and computational power. The data and computation are offloaded to the cloud. However, as the cloud is a distributed service model, this means that the cloud service provider will be a different entity from the application developer and the app owner, and the physical location of data storage and processing may take place in multiple jurisdictions.[348]

App developers may typically also rely on cloud-based services for 'back end services' (hence mobile back-end as a service or MBaas), such as hosting, payment gateways, web analytics, application monitoring and development and testing tools.[349] There may thus be multiple cloud service contracts, and the responsibilities of each cloud service provider

[346] V Weber and A Carblanc, *Cloud computing: The concept, impacts and the role of government policy* (OECD, Paris, 2014) at 11. When an app developer stores data in a data centre over which they retain full control they are utilising a private cloud, but when they permit outsource processing which requires sharing some or all of the data, they may be using a hybrid cloud deployment model.
[347] Ibid at 10.
[348] For further discussion of mobile cloud computing see Anirudh Paranjothi, Mohammad S. Khan and Mais Nijim, 'Survey on Three Components of Mobile Cloud Computing: Offloading, Distribution and Privacy' (2017) 5 *Journal of Computer and Communications* 1–31.
[349] Cameron McKenzie, Jason Tee and Sal Pece 'Mobile Development Takes to the Cloud' Available at cdn.ttgtmedia.com. , accessed on 11 April 2018.

would have to be analysed in terms of the contract and against the applicable legislation, and any code of conduct adhered to by the cloud service provider.[350]

Cloud services are rapidly evolving. Whereas previously each back-end service was incorporated into the app by an API, cloud platforms offering a unified SDK which allows the mobile app to integrate with multiple backend services in the cloud have emerged. An example is the Google Cloud platform.[351]

None of the data protection statutes studied refers expressly to cloud computing, and the relationship between cloud user and cloud provider must be analysed within the legislative framework of the relationship between a responsible party and a processor. This seems to be an approximation of an outsourcing relationship, whereas there may be a need to reconceptualise the cloud computing relationship. For example, IaaS, PaaS and pure data storage, SaaS, service providers would still be classified as processor (or as 'joint' responsible party), whereas a traditional supplier of hardware (sale/rental) would not.[352]

X CONCLUSION

This chapter defined key concepts, role-players and data processing activities in the mobile apps ecosystem. However, despite widespread academic and media concern about privacy risks, we have only a 'rudimentary' understanding of what personal information is collected and how it is processed.[353] Understanding is impeded by the complexity, diversity and lack of transparency around data sharing practices within the mobile ecosystem,[354] which are treated as 'proprietary' information[355] and thus not made public. As such, app developers may

---

[350] As to the development of an approved industry code of conduct, see European Cloud Code of Conduct at 5. Available at https://eucoc.cloud/fileadmin/cloud-coc/files/European_Cloud_Code_of_Conduct.pdf accessed 13 April 2018.
[351] Google LLC., 'Mobile app backend services'.
[352] Hon H Kuan, 'GDPR: Killing cloud quickly?' (*International Association of Privacy Professsionals (IAPP)*, 17 March 2016) <https://iapp.org/news/a/gdpr-killing-cloud-quickly/> accessed 7 March 2018. The accountability of the responsibility party and processor is examined in depth in chapters 4, 5 and 6. A detailed examination of mobile cloud computing is beyond the scope of this dissertation. See further European Commission (Expert group on cloud computing contracts), *Discussion Paper: Meeting of 19 & 20 November 2013* (2013) and EU CLOUD COC, *EU Data Protection Code of Conduct for Cloud Service Providers* (2018).
[353] Yabing Liu and others, 'Identifying Personal Information in Internet Traffic' in *Proceedings of ACM Conference on Online Social Networks* (ACM, Palo Alto, USA 2–3 November 2015).
[354] Ullah (2017).
[355] Liu and others.

themselves be unaware of what data is being collected by third party libraries and SDKS,[356] and hence unable to make appropriate privacy disclosures to app users. Sustained engagement by the Information Regulator with all stakeholders will be essential for a deeper understanding of the issues outlined in this chapter.[357]

[356] Stevens and others.
[357] Binns and others.

CHAPTER 3

'PRIVACY BY (RE)DESIGN' IN ITS INTERNATIONAL, REGIONAL AND NATIONAL CONTEXT

I INTRODUCTION

There is a substantive body of scholarly work on data protection[1] that provides a detailed analysis of the data protection laws of different countries or regions and offers comparative conclusions.[2] The present study builds on that work, without seeking to replicate it.

It proceeds on the assertion that the core data protection principles are broadly similar in their various iterations,[3] although paradoxically the right to privacy, which is foundational to data protection laws, is widely accepted as being understood differently in different cultures.[4] In the premises, the application of high-level principles in any particular

---

[1] For relevant work in a South African context see Anneliese Roos, 'The law of data (privacy) protection: a comparative and theoretical study' (2009), Ray William London, 'Comparative data protection and security law: A critical evaluation of legal standards' (University of South Africa 2013), Ewan Sutherland, 'Digital Privacy in Africa: Cybersecurity, Data Protection & Surveillance' [2018] <http://dx.doi.org/10.2139/ssrn.3201310> accessed 18 April 2020, and Beverley Alice Townsend, 'Privacy and data protection in eHealth in Africa-an assessment of the regulatory frameworks that govern privacy and data protection in the effective implementation of electronic health care in Africa: is there a need for reform and greater regional collaboration in regulatory policymaking?' (University of Cape Town 2017). Also see Anneliese Roos 'Data Protection' in Van der Merwe D (ed) *Information and Communications Technology Law* (2 ed, LexisNexis 2016), Yvonne Burns and Ahmore Burger-Smidt *A Commentary on the Protection of Personal Information Act* (LexisNexis 2018) and the South African Law Reform Commission, *Project 124 'Privacy and data protection'* (2009).

[2] Hazel Grant and others (eds), *Encyclopedia of Data Protection and Privacy* (Sweet & Maxwell 1989 (looseleaf updates)), Lee Bygrave, *Data Privacy Law: An International Perspective* (Oxford Scholarship Online 2014), Rosemary Jay, *Data Protection: Law and Practice* (with 1st supplement, 4 ed, Sweet & Maxwell 2014), Rosemary Jay, *Guide to the General Data Protection Regulation* (Sweet & Maxwell 2017), Christopher Kuner, *Transborder Data Flows and Data Privacy Laws* (OUP 2013) and Christopher Kuner and others (eds), *The EU General Data Protection Regulation (GDPR): A Commentary* (OUP 2020). Also see influential earlier work by Colin J. Bennet, *Regulating privacy : data protection and public policy in Europe and the United States* (Cornell University Press 1992) Lee A. Bygrave, *Data Protection Law−Approaching Its Rationale, Logic and Limits* (Kluwer International 2002), Raymond Wacks, *Personal Information: Privacy and the Law* (OUP 1994), David Bainbridge, *Data Protection Law* (2 edn, XPL 2005), Peter Carey and Bridget Treacy, *Data protection : a practical guide to UK and EU law* (4 edn, OUP 2015) , Wayne Madsen, *Handbook of Personal Data Protection* (Palgrave Macmillan 1992), and Ian Walden, 'Data Protection' in Chris Reed and John Angel (eds), *Computer Law* (5 ed, OUP 2003).

[3] Roos at 21 citing Bygrave at 12. Also see South African Law Reform Commission, ch. 4.

[4] Joel R. Reidenberg, 'Resolving Conflicting International Data Privacy Rules in Cyberspace' (2000) 52 *Stan L Rev* 1315–1371 at 1318. Also see generally Alan F. Westin, *Privacy and Freedom* (Athenum 1967) and David H. Flaherty, *Protecting Privacy in Surveillance Societies: The Federal Republic of Germany, Sweden, France, Canada, and the United States* (The University of North Carolina Press 1989) and Fred H. Cate, *Privacy in the Information Age* (Brookings Institution Press 2000).

society may vary considerably, even among different member states of the European Union,[5] and within South African legal literature and case law.[6] However, the chapter goes beyond earlier works by providing a critical analysis and discussion of how the core data protection principles relate to PbD. The chapter commences with a description of the core data protection principles with reference to their international, regional and national context. Next, the conceptual framework of privacy by design (PbD) is set out. The foundational principles of PbD are described and their relationship to the core data protection principles is explained. PbD is the 'concept of engineering privacy directly into the design of new technologies, business practices and networked infrastructure, in order to achieve the doubly-enabled pairing of functionality and privacy'.[7] Privacy by design underpins both the General Data Protection Regulation (2016) (GDPR)[8] in the European Union (EU), and the Protection of Personal Information Act (2013) (POPIA)[9] in South Africa.

In the study presented in this dissertation, an 'app-developer-centric' approach is taken. Such an approach is described in a recent meta-study which advocates for empirical research to better understand the mobile application ecosystem and how PbD principles can be implemented in the field of mobile application development.[10] Specifically the roles and responsibilities of the app developer during the app development process and data lifecycle are carefully considered, in order to understand the app developer's perspective on how abstract legal principles can be implemented in practical, real world contexts.[11]

---

[5] Walden at 419.
[6] For discussion in a South African context see David McQuoid-Mason, 'Privacy' in Stuart Woolman and Michael Bishop (eds), *Constitutional Law of South Africa*, vol 3 (2 ed, Juta 2014), and Johann Neethling, *Persoonlikheidsreg* (4 edn, Lexis Nexis 2013) and Johann Neethling, 'The Concept of Privacy in South African Law' (2005) 122 *SALJ* 18–22.
[7] A Cavoukian and M Prosch, *The Roadmap for Privacy by Design in Mobile Communications: A Practical Tool For Developers, Service Providers, and Users* (Toronto, ON, Canada: Office of the Privacy Commissioner, Ontario, Canada, 2010) at 3.
[8] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA OJ L 119, 4.5.2016 (EU General Data Protection Regulation; GDPR).
[9] Protection of Personal Information Act 4 of 2013 (POPIA).
[10] European Union Agency For Network and Information Security (ENISA), *Privacy and Data Protection in Mobile Applications: A Study on the App Development Ecosystem and the Technical Implementation of GDPR* (November 2017).
[11] Ibid at 5.

II CORE DATA PROTECTION PRINCIPLES

The set of eight core data protection principles articulated in the OECD Privacy Guidelines in 1980[12] evolved from the collective, growing concern among Western nations with the extensive inroads upon individual privacy made possible by the advent of computing.[13] The principles themselves were drawn from the existing legislation enacted in OECD member states, which shared a common identification of the 'elementary components' of data protection.[14] The principles also draw upon the fair information practice principles (FIPs) adopted in the US[15] as the basis for the 1974 Privacy Act.[16] The principles remain unchanged in the 2013 OECD Privacy Framework.[17]

From the outset, the OECD Guidelines have had two distinct and competing[18] goals: to uphold the individual's fundamental human right to privacy, and to prevent serious disruptions to trade by restricting the free-flow of personal data across national frontiers.[19] Interestingly, while articulating both goals as 'fundamental values',[20] the 2013 Guidelines

---

[12] *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980) ss 7–15.
[13] South African Law Reform Commission at 143, as part of a comprehensive discussion in chapter 4.
[14] OECD, Explanatory memorandum para 2.
[15] As to the historical background to the conceptualisation of these principles in a 1973 report of the Department of Health Education and Welfare (HEW) and their enactment and shortcomings in the United States see Fred H. Cate, 'The Failure of Fair Information Practice Principles ' in Jane K. Winn (ed), *Consumer Protection in the Age of the 'information Economy'* (Ashgate 2006). Ironically the same HEW Dept. was at the forefront of developing computer matching programs in the late 1970s: Flaherty at 344.
[16] The Privacy Act of 1974, 5 U.S.C. § 552a (2018). This Act applies to government use of personal information. As to private use of personal information and the FIPPS see further discussion in chapter 4.
[17] OECD, *Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data* (C(80)58/FINAL, as amended on 11 July 2013 by C(2013)79, 2013) ss 7–15.
[18] OECD, recital. Although the goals are certainly not mutually exclusive, there will often be tension between them. As to the tension between governments' obligation to uphold the right to privacy and governments' interests in data as a surveillance tool, see Flaherty at 13–14. It must be said that a similar tension arises in relation to the 'surveillance' potential of large data stores held by corporate entities and the 'accountability' principle that obliges data controllers to respect data subject privacy.
[19] OECD states in the preface to the guidelines that: 'The development of automatic data processing, which enables vast quantities of data to be transmitted within seconds across national frontiers, and indeed across continents, has made it necessary to consider privacy protection in relation to personal data. … there is a danger that disparities in national legislations could hamper the free flow of personal data across frontiers; [and] … could cause serious disruption in important sectors of the economy, such as banking and insurance. … OECD Member countries considered it necessary to develop Guidelines which would help to harmonise national privacy legislation and, while upholding such [fundamental] human rights, would at the same time prevent interruptions in international flows of data'.
[20] Ibid. The recital to the 1980 Guidelines refers to privacy and the free flow of information as 'fundamental *but competing* values' (own emphasis).

reflect that personal data is 'increasingly a valuable commodity'.[21] This, it is observed, appears to mark the growing importance of 'digital transformation' as a driver of economic and social advancement[22] and a recognition that 'digital technologies and knowledge-based capital is [sic] profoundly transforming our societies'.[23] Underlying the approach of the OECD is thus an inherently positive view of the potential of the digital economy, tempered by recognition that, inter alia, transformation must respect the rule of law and human rights.[24]

The data protection principles set out in the OECD Guidelines are not discrete but are interconnected and partially overlapping,[25] and are therefore best studied as a whole.[26]

'1. Collection Limitation Principle

There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

2. Data Quality Principle

Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up to date.

3. Purpose Specification Principle

The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

4. Use Limitation Principle

---

[21] The recital to the 2013 OECD Privacy Guidelines refers to privacy and the free flow of information as 'fundamental' values. It recognises that 'more extensive and innovative uses of personal data bring greater economic and social benefits, but also increase privacy risks.'

[22] OECD (Committee on Digital Economy Policy), *Resolution of the Council [C(2018)141, and C/M(2018)xx, item xxx] Draft Resolution of the Council renewing and revising the mandate of the Committee on Digital Economy Policy* (2018).

[23] OECD, *Cancún Ministerial Declaration on the Digital Economy* (2016).

[24] Ibid.

[25] OECD, *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, Explanatory Memorandum para 50.

[26] South African Law Reform Commission at 161.

Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Paragraph 9 except:

a) with the consent of the data subject; or
b) by the authority of law.

5. Security Safeguards Principle

Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data.

6. Openness Principle

There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.

7. Individual Participation Principle

Individuals should have the right:

a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to them;
b) to have communicated to them, data relating to them:
    i. within a reasonable time;
    ii. at a charge, if any, that is not excessive;
    iii. in a reasonable manner; and
    iv. in a form that is readily intelligible to them;
c) to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and
d) to challenge data relating to them and, if the challenge is successful, to have the data erased, rectified, completed or amended.

8. Accountability Principle

A data controller should be accountable for complying with measures which give effect to the principles stated above.'[27]

III DATA PROTECTION IN ITS INTERNATIONAL, REGIONAL AND NATIONAL CONTEXT

The Council of Europe (COE) is an international organisation comprising 47 member states from Europe, including all 28 members States of the European Union (EU).[28] It began work on data privacy in the late 1960s, commissioning a study into whether the European Human Rights Convention and domestic laws provided sufficient protection to the right to privacy in the advent of automated data banks made possible by computers.[29] In 1981 it adopted the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data.[30] The Convention is to be read with a 2001 Protocol[31] and a 2018 protocol that is not yet in force.[32]

Convention 108, like the OECD Guidelines, is principles based and technology neutral.[33] It sets out goals and data protection principles that are broadly similar to those set out in the OECD Guidelines. The Convention has been ratified without reservation by all 47

---

[27] OECD, *Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data* (C(80)58/FINAL, as amended on 11 July 2013 by C(2013)79, 2013) ss 7–15, which remain unchanged from OECD, *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980) ss 7–15.

[28] Council of Europe, 'Our Member States' <https://www.coe.int/en/web/about-us/our-member-states> accessed 1 June 2019. The United States, Canada, Mexico, Japan, Israel and the Holy See have observer status. Also see Christopher Kuner, *European Data Privacy Law and Online Business* (OUP 2003) at 36.

[29] Council of Europe, *Explanatory Report to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data* (1981) para 4. The report sets out a comprehensive history of the COE's work on data privacy and close co-operation with the OECD and its 4 non-European member States (Australia, Canada, Japan, and the United States) who had observer status on the COE.

[30] COE Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (COE Convention 108) ETS 108 (1981, as amended in 1999).

[31] Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding supervisory authorities and transborder data flows (entry into force 1 July 2004) ETS 181 (2001). This protocol provides for the creation of independent supervisory authorities and requires adequate safeguards for the transfer of data to States or organisations that were not subject to the Convention.

[32] Council of Europe Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, CETS 223 (2018). It will enter into force on 11 October 2023, provided there are 38 parties to the protocol, or earlier if ratified by all parties to Convention 108.

[33]Council of Europe, *128th Session of the Committee of Ministers* (Elsinore, Denmark, 17–18 May 2018) – *Ad hoc Committee on Data Protection (CAHDATA) – Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108) – Explanatory report.* (CM(2018)2-addfinal, 2018) para 2 and 12.

Member States, most recently entering into force on 1 September 2016 in Turkey.[34] However, it is also open for adoption by non-member States, and has entered into force in eight non-member States, including the African states of Cabo Verde, Mauritius, Morocco, Senegal and Tunisia.[35]

The core data protection principles are also reflected in regional data protection instruments.[36] The Asia-Pacific Economic Cooperation (APEC) Privacy Framework was developed in 2005[37] and updated in 2015.[38] The US is a member state of APEC.[39] However, the federal and state laws discussed in chapter 4[40] reflect the pared-down FIPPS, and not the full eight data-processing principles.

In the EU, the COE Convention is binding on member states, and its principles are similarly reflected in GDPR (as well as in the earlier Data Protection Directive,[41] and in national data protection laws in member States).[42]

In South Africa, the Convention and the OECD Guidelines were taken into close consideration in the drafting of POPIA, being regarded as 'crucial' instruments that have had a 'profound effect' in shaping national data protection laws.[43] Additionally, the regional frameworks for data protection are set out in the African Union (AU) Convention on Cybercrime and Personal Data Protection,[44] the Data Protection Guidelines published on

---

[34] Council of Europe, 'Chart of signatures and ratifications of Treaty 108' <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/signatures?p_auth=783d1rIE> accessed 1 June 2019.

[35] Ibid. The other non-member States who have acceded to the Convention are the South American countries of Argentina, Mexico and Uruguay.

[36] A comparative study of those instruments falls outside the scope of this study.

[37] APEC, *APEC Privacy Framework* (APEC#205-SO-012, 2005).

[38] APEC, *APEC Privacy Framework (2015)* (APEC#217-CT-019, 2017).

[39] APEC, 'List of APEC member states' <https://www.apec.org/About-Us/About-APEC/Member-Economies.aspx> accessed 26 October 2019.

[40] The Children's Online Privacy Protection Act of 1998, 15 U.S.C. §§ 6501 - 6506 (2018) (COPPA), The Online Privacy Protection Act of 2003, Cal. Bus. & Prof. Code §§ 22575–22579 (2004) and The California Consumer Privacy Act of 2018, Cal. Civ. Code §§ 1798.100 - 1798.199 (CCPA).

[41] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (Data Protection Directive) OJ 1995 L 281/31, 23.11.1995.

[42] A comparative analysis of member State laws is beyond the scope of this dissertation.

[43] South African Law Reform Commission at 7.

[44] African Union Convention on Cyber Security and Personal Data Protection (Malabo, 2014). The Convention is not yet in force, having only been ratified by 8 nations. South Africa is not a signatory to the Convention. African Union (AU) 'List of countries which have signed, ratified/acceded to the African Union Convention on Cyber Security and Personal Data Protection' (18 June 2020) < https://au.int/sites/default/files/treaties/29560-sl-african%20union%20convention%20on%20cyber%20security%20and%20personal%20data%20protection.pdf> accessed 1 August 2020.

9 May 2018,[45] and the Southern African Development Community (SADC) Model Law on Data Protection.[46]

IV THE CONCEPTUAL FRAMEWORK OF PRIVACY BY DESIGN (PBD)

The rapid development of technology and the new uses for personal data are proving a challenge to the application of data protection laws.[47] The conceptual framework of PbD has been widely accepted as an approach that can address this challenge. The concept was first developed in the 1990s.[48] In 2010, the 32nd International Conference of Data Protection and Privacy Commissioners adopted a unanimous resolution endorsing PbD,[49] and the concept has continued to grow in popularity.[50]

PbD comprises seven foundational principles that are explained in Table 3 below.

TABLE 3. THE SEVEN FOUNDATIONAL PRINCIPLES OF PRIVACY BY DESIGN

Principle	**Description**
1. ***Proactive***, not Reactive; ***Preventative***, not Remedial	The *Privacy by Design* approach is characterised by proactive rather than reactive measures.
2. Privacy as the Default Setting	No action is required on the part of the individual to protect their privacy − it is built into the system, *by default*.

[45] Internet Society (ISOC) and Commission of the African Union, *Personal Data Protection Guidelines for Africa* (2018). See discussion at 9–10 on convergence of a set of core data protection principles.
[46] Southern Africa Development Community (SADC), *Draft SADC Model Law on Data Protection* (2011). Also see International Telecommunications Union (ITU), *Data Protection: Southern African Development Community (SADC) Model Law* (Geneva, 2013). For similar regional initiatives see Economic Community of West African States (ECOWAS) Supplementary Act on Personal Data Protection within ECOWAS (Abuja, 2010) and East African Community (EAC), *Draft EAC Framework for Cyberlaws* (November 2008).
[47] OECD, *The OECD Privacy Framework* (2013) at 66.
[48] Ann Cavoukian, 'Privacy by Design: Origins, Meaning, and Prospects for Assuring Privacy and Trust in the Information Era' in George O.M. Yee (ed), *Privacy Protection Measures and Technologies in Business Organizations: Aspects and Standards* (Aptus Research Solutions Inc. and Carleton University, Canada 2012) at 16.
[49] A Cavoukian, *Privacy by Design Strong Privacy Protection – Now, and Well into the Future a Report on the State of PbD to 33rd International Conference of Data Protection and Privacy Commissioners* (Toronto, ON, Canada: Office of the Privacy Commissioner, Ontario, Canada, 2011) at 6.
[50] Kirsten Martin and Katie Shilton, 'Putting Mobile Application Privacy in Context: An Empirical Study of User Privacy Expectations For Mobile Devices' (2016) 32 *The Information Society* 200–216 at 201.

3. Privacy ***Embedded*** into Design	*Privacy by Design* is embedded into the design and architecture of IT systems and business practices. It is not bolted on as an add-on, after the fact.
4. Full Functionality – ***Positive-Sum***, not Zero-Sum	*Privacy by Design* seeks to accommodate all legitimate interests and objectives in a positive-sum "win-win" manner, not through a dated, zero-sum approach, where unnecessary trade-offs are made.
5. End-to-End Security – ***Full Lifecycle Protection***	*Privacy by Design*, having been embedded into the system prior to the first element of information being collected, … ensures cradle-to- grave, secure lifecycle management of information, end-to-end.
6. ***Visibility*** and ***Transparency*** – Keep it ***Open***	Its component parts and operations remain visible and transparent, to both users and providers alike.
7. ***Respect*** for User Privacy – Keep it ***User-Centric***	Above all, *Privacy by Design* requires architects and operators to keep the interests of the individual uppermost by offering such measures as strong privacy defaults, appropriate notice, and empowering user-friendly options.

Source: Cavoukian & Prosch 2010:5-6 (e.i.o.)

The seven foundational principles of PbD are closely aligned to the core data protection principles. That relationship, drawing on the framework developed by Cavoukian,[51] is summarised in Table 4 below.

[51] A Cavoukian, *Privacy by Design The 7 Foundational Principles Implementation and Mapping of Fair Information Practices* (Information and Privacy Commissioner, Ontario, Canada, 2010).

TABLE 4 MAPPING PBD TO DATA PROTECTION PRINCIPLES

PbD Principle	**FIPs**	**Data Protection Principles**	**Practical Approach**
Proactive and Preventative Approach	---	**Accountability** **Security**	A 'proactive, systematic and innovative' approach to implementing the highest possible standards of privacy and security is applied throughout the organisation and the ecosystem.[52]

[52] Cavoukian at 3. The author has not explicitly 'mapped' this PbD principle to the FIPs, on the basis that a proactive approach may go beyond legal standards.

Privacy as the Default	**Purpose Specification**[53] **Collection Limitation**[54] **Data Minimisation**[55] **Use, Retention and Disclosure Limitation**[56]	**Purpose Specification** **Collection Limitation**[57] **Use Limitation**[58]	In line with a 'presumption of privacy'[59] and a 'precautionary approach',[60] default settings are 'the most privacy protective'[61]

[53] Defined by Cavoukian at 3 as follows: 'the purposes for which personal information is collected, used, retained and disclosed shall be communicated to the individual (data subject) at or before the time the information is collected. Specified purposes should be clear, limited and relevant to the circumstances'.
[54] Defined by Cavoukian at 3 as follows: 'the collection of personal information must be fair, lawful and limited to that which is necessary for the specified purposes.'
[55] Defined by Cavoukian at 3 as follows: 'the collection of personally identifiable information should be kept to a strict minimum. The design of programs, information and communications technologies, and systems should begin with non-identifiable interactions and transactions, as the default. Wherever possible, identifiability, observability, and linkability of personal information should be minimized'.
[56] Defined by Cavoukian at 3 as follows: 'the use, retention, and disclosure of personal information shall be limited to the relevant purposes identified to the individual, for which he or she has consented, except where otherwise required by law. Personal information shall be retained only as long as necessary to fulfill the stated purposes, and then securely destroyed'.
[57] Indirectly the OECD Guidelines refer to data minimisation by virtue of the principle of 'collection limitation', namely the principle that '[t]here should be limits to the collection of personal data', which is supplemented by the 'data quality' principle which requires that data 'should be relevant to the purposes for which they are to be used'.
[58] The 'use limitation' principle applies to both use and disclosure of personal data. Although under the principle of data subject participation a data subject can require a controller to delete personal data concerning him or her, the OECD Guidelines do not contain any provision limiting data retention per se, and requiring its automatic deletion once it has served its purpose.
[59] Cavoukian at 3. While the term is not defined by the author, it could mean that the app developer presumes that the user expects privacy, the law presumes that the user is entitled to privacy, and the user can presume that their privacy is protected unless it clear to them that the personal information is needed and how it will be used.
[60] Cavoukian at 3. While the term is not defined by the author, its inclusion under the heading of 'default settings' suggests that to avoid any doubt that the data subject is aware of and consents to the collection or use of personal information, the default setting should be to require the data subject to actively permission the first collection or use.
[61] Cavoukian at 3. Again, although the terms used might suggest otherwise, it is clear from the overall tenor of PbD that user privacy is not to be at the expense of full functionality. PbD calls for innovative design that can provide that functionality while protecting privacy to the fullest extent reasonably possible.

Privacy Embedded into Design	---	**Purpose Specification** **Collection Limitation** **Use Limitation**	Systematic adoption of 'accepted standards and frameworks',[62] subject to independent review or audit. and internal privacy impact assessments. The aim is to demonstrate minimal privacy impacts considering anticipated use, and possibilities for misconfiguration or error.
Full Functionality – Positive Sum not Zero Sum	---	**Balance rights and legitimate interests of all parties**	Clearly document interests, objectives and desired functions Innovative solutions to embed privacy whilst permitting full functionality
End to End Lifecycle Protection	**Security**[63]	**Security** **Information quality** **Accountability**	Have 'no gaps in protection or accountability.'[64] Apply recognised security standards, including secure destruction, encryption, access controls and logs, to ensure 'confidentiality, integrity and availability' of personal data 'across the entire domain and

[62] Cavoukian at 3, recognises that PbD requires consideration of the 'broader context' and consultation of 'all stakeholders and interests', i.e. it is an eco-system wide approach. However, she also calls for creative invention of new alternatives where existing solutions are unacceptable from the privacy perspective.
[63] Cavoukian at 4 'maps' this PbD principle to all FIPs but identifies security as particularly important. She defines security as follows: 'Entities must assume responsibility for the security of personal information (generally commensurate with the degree of sensitivity) throughout its entire lifecycle, consistent with standards that have been developed by recognized standards development bodies.'
[64] Cavoukian at 4.

			throughout the life-cycle of the data.'[65].
Visibility and Transparency	**Accountability**[66] **Openness** **Compliance**[67]	**Accountability** **Openness**	Operate 'according to stated promises and objectives'.[68] Use independent trust verification measures.
Respect for User Privacy	**Consent** **Accuracy** **Access** **Compliance**	**Use Limitation** **Information Quality** **Data Subject Participation**	Technology interfaces and organisational processes and procedures should be user-centric and user-friendly

Source: Col 1, 2 and 4: summarised from Cavoukian (2010) 2–5. Col 3: inserted by researcher drawing on OECD Guidelines.

While Cavoukian asserts that PbD imposes a significantly higher standard than that encompassed by FIPPS, of notice, choice, and access,[69] this claim is doubted by others.[70] Moreover, in the case of the broader set of core data protection principles set out in the OECD Guidelines, which underpin POPIA and GDPR, there appears to be almost complete overlap, as illustrated in Table 4 above.

[65] Cavoukian at 4.
[66] Cavoukian at 5 aligns this with all FIPs but singles out accountability, openness and compliance as especially apposite. Accountability is defined by Cavoukian as follows: 'The collection of personal information entails a duty of care for its protection. Responsibility for all privacy-related policies and procedures shall be documented and communicated as appropriate and assigned to a specified individual. When transferring personal information to third parties, equivalent privacy protection through contractual or other means shall be secured.'
[67] With respect to compliance Cavoukian at 4, refers to mechanisms for enforcement and redress, including organisationa' procedures for handling complaints and monitoring compliance.
[68] Cavoukian at 5. Privacy policies and procedures must be documented, kept up to date and available, and assigned to the responsibility of a person within the organisation. Contractual safeguards must be implemented when disclosing personal information to third parties.
[69] See further detailed discussion in chapter 4.
[70] Ira S Rubinstein and Nathaniel Good, 'Privacy by Design: A Counterfactual Analysis of Google and Facebook Privacy Incidents' (2013) 28 *Berkeley Tech LJ* 1333–1414 at 1337 asserts that the PbD principles offer no further practical assistance than the FIPPS.

V THE NATURE OF PRIVACY BY DESIGN

PbD is not in fact a new, self-standing legal principle but is a systems engineering approach that can help to translate legal principles into application within the design of IT systems.[71] This much is clear when one examines the origins of the concept of PbD. The problem in practice that PbD originally sought to address was the misconception that security was equivalent to privacy.[72] The 1995 report recorded that:

> *'When organizations are asked what measures they have in place to protect privacy, they usually point to their efforts at keeping information secure. While the use of security measures to prevent unauthorized access to personal data is a very important component of privacy, it does not equal privacy protection. The latter is a much broader concept which starts with the questioning of the initial collection of the information to ensure there is a good reason for doing so and that its uses will be restricted to legitimate ones that the data subject has been advised of. Once the data have been collected, security and confidentiality become paramount. Effective security and confidentiality will depend on the implementation of measures to create a secure environment.'*[73]

As outlined above, security is one of eight core data protection principles. What the report highlighted was that the IT sector appeared to have lost sight of the other seven, or perhaps to lack the means of translating the legal concepts into actionable systems engineering goals. Hence the focus of the report was on describing privacy-enhancing technologies (PETs)

---

[71] A brief consideration of the origins of PbD, and the intention behind that report, is necessary as the introduction of article 25 on data protection by design and by default into the GDPR raises the question whether PbD is a new, self-standing legal principle that ought to be expressly introduced by amendents to other data protection statutes such as POPIA. This is discussed in depth in chapters 8 and 9. For a discussion of systems engineering in relation to PbD see Jeroen van Rest and others, 'Designing Privacy-by-Design' [2014] *Privacy Technologies and Policy* 55. Systems Engineering may be defined as 'a transdisciplinary and integrative approach to enable the successful realization, use, and retirement of engineered systems, using systems principles and concepts, and scientific, technological, and management methods. We use the terms "engineering" and "engineered" in their widest sense: "the action of working artfully to bring something about". "Engineered systems" may be composed of any or all of people, products, services, information, processes, and natural elements'. International Council on Systems Engineering (INCOSE), 'What is Systems Engineering?' (2019) <https://www.incose.org/systems-engineering> accessed 29 September 2019. Mobile system engineering is a specialised sub-set of this broader transdisciplinary field. Also see A Cavoukian, Stuart Shapiro and R. Jason Cronk, *Privacy Engineering: Proactively Embedding Privacy, by Design* (IPC, Ontario Canada, 2014) at 2.

[72] About this there is a larger literature, much of which reflects the same misconception and thus reflects a debate about whether privacy and security are the same concept.

[73] Information and Privacy Commissioner Ontario Canada and Registratiekamer The Netherlands, section 1.2.

available at that time, and emphasising the importance of anonymity, as a means of minimising the amount of personal data collected.[74]

On closer analysis of the report,[75] it is absolutely clear that PbD was not put forward as a new legal principle; nor did it call for the amendment or extension of existing data protection principles. Instead, it put forward a workable systems approach to adopting PETs to implement existing data protection principles in the design of information technology systems. Over time, this approach has evolved from PETs to one that also encompasses privacy within organisations, IT systems architecture and ecosystems.[76]

This approach was developed further by Cavoukian, who emphasised in *Privacy by Design: The 7 Foundational Principles*, published in 2009, that the concept of privacy by default was a 'PET-*Plus*' approach.[77] In such an approach, organisations adopt privacy as a default organisational modus operandi. The goal is to protect privacy while providing full functionality of the system.[78] The advantage to the data subject is control over their personal data, while the organisation gains a competitive advantage[79] premised on the assumption that consumers exhibit a preference for applications that preserve their privacy.[80] As will be discussed further below, the legal principles of accountability and data minimisation are central to PbD.

---

[74] Ibid. For a fuller discussion of the origins of PETs see European Network and Security Agency, *Privacy and Data Protection by Design: From Policy to Engineering* (2014) at 5.
[75] Information and Privacy Commissioner Ontario Canada and Registratiekamer The Netherlands, section 1.4.
[76] Cavoukian at 171.
[77] A Cavoukian, 'Privacy by Design The 7 Foundational Principles' (2009 (revised January 2011)) <https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf> accessed 26 September 2019.
[78] Ibid.
[79] Ibid.
[80] As an example, Apple takes such an approach. The underlying assumptions rest on studies showing consumer concerns about privacy, but whether this translates into a competitive advantage for companies adopting privacy measures is open to doubt given high levels of consumer ignorance, and apathy, towards privacy protection, the lack of any competitive market for PETs, and entrenched systemic factors. European Data Protection Supervisor (EDPS), *Opinion of the European Data Protection Supervisor on the Communication from the Commission to the European Parliament and the Council on the follow-up of the Work Programme for better implementation of the Data Protection Directive* (2007/C 255/01, 2007) at 406. Also see generally Lee A Bygrave, 'Data Protection by Design and by Default: Deciphering the EU's Legislative Requirements' (2017) 4 *Oslo Law Review* 105–120, referring to the earlier work on privacy 'markets' in Alessandro Acquisti, Curtis Taylor and Liad Wagman, 'The Economics of Privacy' (2016) 54 *Journal of Economic Literature* 442–492 at 473. On behaviour economics see van Rest and others at 57. On competition issues, see Maurice E Stucke and Allen P Grunes, *Big Data and Competition Policy* (OUP 2016). For further discussion see Lee A. Bygrave, 'Hardwiring Privacy' in Roger Brownsword, Eloise Scotford and Karen Yeung (eds), *The Oxford Handbook of Law, Regulation, and Technology* (OUP 2017) at 762–763.

IX PRIVACY BY (RE)DESIGN

Privacy by (re)design is described by Cavoukian as an extension of the PbD approach to apply to legacy systems and existing operations.[81] It flows from the recognition that the principle of designing for privacy from the outset cannot be applied to existing systems. Instead, it calls for PbD's objective of achieving the highest standard of privacy protection to be actioned through the redesign of systems.

The process of implementing privacy by (re)design outlined by Cavoukian can also be mapped to the core data protection principles in data protection laws. She recommends that companies should 'review their risk mitigation strategies, existing systems, and processes'[82] and redesign and 'revive' their systems accordingly. Under both POPIA and GDPR, the accountability principles impose a continuous obligation to ensure compliance with data protection principles at each stage of processing and throughout the data lifecycle.[83] As Cavoukian's report illustrates, an assumption that the collection or storage of particular personal information is necessary may appear unfounded upon later review.[84] The fact that the collection or storage may initially have been necessary or reasonable will not avail a responsible party. Section 10 of POPIA stipulates that '[p]ersonal information may only be processed if, given the purpose for which it is processed, it is adequate, relevant and not excessive'. The principle of minimality is expressed in the present tense, implying that the condition imposes a continuous limitation upon processing. If, in the light of advances in technological or business processes, the purpose can now be achieved without processing personal information, then the processing would be 'excessive' and consequently unlawful.[85]

Cavoukian suggests that PbD can be implemented when new components are added, but that existing components 'may need to be wholly redesigned to reflect privacy objectives'.[86] However, apart from a fleeting assertion that implementing PbD across

---

[81] Cavoukian and Popa. Also see A Cavoukian, *Privacy by Design in Law, Policy and Practice A White Paper for Regulators, Decision-makers and Policy-makers* (Information and Privacy Commissioner, Ontario, Canada, 2011) at 26.
[82] Cavoukian and Popa at 4.
[83] POPIA s 8 and GDPR art 5(2).
[84] Cavoukian and Popa at 4.
[85] Similarly, see GDPR art 5, which is expressed in the present tense.
[86] Cavoukian and Popa at 4.

ecosystems can foster consumer trust,[87] the question of how an ecosystem is redesigned, and the responsibility of the parties identified in chapter 2 as gatekeepers to that ecosystem, and third parties, is not discussed.[88] A comprehensive literature review has revealed a dearth of literature on the implementation of PbD in relation to information system ecosystems in general, and third-party processing in particular.[89] It is against that background that a comprehensive legal analysis of principles central to an effective PbD approach must be analysed.

VI PRIVACY BY DESIGN AND THE ACCOUNTABILITY PRINCIPLE

What sets PbD apart is that it is a proactive approach. Legislation typically responds to data breaches by imposing sanctions after the fact for the consequences of failing to implement the data protection principles. PbD requires app developers to 'design new applications with privacy in mind right from the outset, and throughout the process and prototyping'.[90] However, while legislation cannot penalise a failure to be 'proactive' in the absence of some demonstrable failure to adhere to enforceable conditions for lawful processing of data, the accountability principle plays a key role in requiring a responsible party to take steps proactively to protect personal information, and thus avoid legislative and regulatory action for non-compliance.

Cavoukian's own definition of accountability as a 'duty of care' lends credit to the argument that PbD is not only compatible with the core data protection principles, but indeed that it cannot be legally enforced beyond the content of those principles. A duty of care is synonymous with a legal duty, either grounded in statute, or common law, and may also refer

---

[87] Cavoukian, *Privacy by Design in Law, Policy and Practice A White Paper for Regulators, Decision-makers and Policy-makers* at 13.

[88] The liability of platforms is a growing area of legal scholarship. See e.g. Katie Shilton and Daniel Greene, 'Linking Platforms, Practices, and Developer Ethics: Levers for Privacy Discourse in Mobile Application Development' (2019) 155 *Journal of Business Ethics* 131–146, OECD, *An Introduction to Online Platforms and Their Role in the Digital Transformation* (2019), Terry Flew, 'The Platformized Internet: Issues for Internet Law and Policy' (2019) 22 *Journal of Internet Law* 3–16, Robert Gorwa, 'What is Platform Governance?' (2019) 22 *Information, Communication & Society* 854–871, Daniel Greene and Katie Shilton, 'Platform Privacies: Governance, Collaboration, and the Different Meanings of "Privacy" in iOS and Android Development' (2018) 20 *New Media & Society* 1640–1657 and Sonia K Katyal and Leah Chan Grinvald, 'Platform Law and the Brand Enterprise' (2017) 32 *Berkeley Tech LJ* 1135–1182 (in relation to trademark and copyright law).

[89] See chapter 1, section VI. Also see Christian Kurtz and Martin Semmann, 'Privacy by Design to Comply with GDPR: A Review on Third-Party Data Processors' (Twenty-fourth Americas Conference on Information Systems, New Orleans, 2018).

[90] Cavoukian and Prosch at 18.

in Cavoukian's usage to a contractual duty.[91] However desirable it may be from a moral or societal perspective for individuals to act in service of the interests of others, the law will refrain from imposing a duty to do so unless the legal convictions of the community require it.[92]

The introduction of PbD originated as part of three issues raised under the broader theme of 'ensuring that data controllers put in place effective policies and mechanisms to ensure compliance with data protection rules' through the principle of accountability.[93]

While PbD was not incorporated expressly in the 1995 European Data Protection Directive,[94] a PbD approach was impliedly required for compliance with the data protection principles contained therein.[95] This was underscored by recital 46, which required that technical and organisational measures to implement data protection must be taken both at the time of the design of the system and at the time of the processing.[96] It is therefore instructive

---

[91] Cavoukian at 4 states that under a PbD approach all parties are 'operating according to the stated promises and objectives', which would include terms in bilateral contracts and representation in privacy policies or terms of use, which are imposed as contractual terms on the user of the product or service.

[92] The classic formulation of this principle that a legal duty to act exists only when imposed by the legal convictions of the community ('die regsoortuiging van die gemeenskap') is set forth in *Minister Van Polisie v Ewels* 1975 (3) SA 590 (A) at 596H–597B/C.

[93] These issues were the mandatory appointment of a Data Protection Officer, mandatory data protection Impact Assessment and concretising PbD. The report states at 11–12: 'The Commission will therefore explore ways of ensuring that data controllers put in place effective policies and mechanisms to ensure compliance with data protection rules…Promoting the use of Privacy Enhancing Technologies (PETs), as already pointed out in the 2007 Commission Communication on the issue, as well as of the 'PbD' principle could play an important role in this respect, including in ensuring data security'. As to what PbD means, the report simply states (at 12): 'The Commission will examine the following elements to enhance data controllers' responsibility … the concept of "PbD" and its concrete implementation, whereby data protection compliance would be embedded throughout the entire life cycle of technologies and procedures, from the early design stage to their deployment and use'. Footnote 30 provides some clarification: 'On PETs see: Communication from the Commission to the European Parliament and the Council on Promoting Data Protection by Privacy Enhancing Technology (PETs) – COM (2007) 228. The principle of "PbD" means that privacy and data protection are embedded throughout the entire life cycle of technologies, from the early design stage to their deployment, use and ultimate disposal. This principle features inter alia in the Commission Communication on 'A Digital Agenda for Europe' – COM (2010) 245'. European Commission, *Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the regions: "A Comprehensive Approach on Data Protection in the European Union"* (COM(2010) 609 final).

[94] For obvious reasons in that, when the report was issued in 1995, Data Protection Directive 95/46/EC had not been finalised.

[95] For detailed discussion of the approach to PbD in the EU see chapter 8.

[96] Data Protection Directive 95/46/EC rec. 46 provides: 'Whereas the protection of the rights and freedoms of data subjects with regard to the processing of personal data requires that appropriate technical and organizational measures be taken, both at the time of the design of the processing system and at the time of the processing itself, particularly in order to maintain security and thereby to prevent any unauthorized processing; whereas it is incumbent on the Member States to ensure that controllers comply with these measures; whereas these measures must ensure an appropriate level of security, taking into account the state of the art and the costs of their implementation in relation to the risks inherent in the processing and the nature of the data to be protected'.

that these provisions are retained in GDPR and have been strengthened by the introduction of an express accountability principle in article 5(2).

VII PRIVACY BY DESIGN AND THE PRINCIPLE OF MINIMALITY

The background to the 1995 report was a study[97] of conventional information systems and communications technologies for curbing the use of identifying data, particularly within information systems. The study revealed that while the data minimisation principle requires that the least amount of personal information possible be collected, in practice this did not happen. As much data as possible was collected.[98] The report called for 'a paradigm shift away from a "more is better" mind-set to a minimalist one'.[99]

This was not new: data protection laws have called for data minimisation under different guises from their earliest recitations.[100] In PbD discourse, Cavoukian uses the term to mean that 'the collection, use, disclosure and retention of personal information should be minimized wherever, and to the fullest extent, possible'.[101] Under POPIA and GDPR it is further encapsulated in the foundational premise that processing must have a lawful and reasonable justification. In other words, 'the default rule underpinning [the legislation] is that personal data should, in general, *not* be processed, so that a high level of protection of the right to privacy is ensured'.[102]

The rationale for PbD is also premised upon the principle of openness (transparency) and individual participation (access and control):

---

[97] Outlined in volume 2 of the report.

[98] This still appears to be the case. For a small study of South African mobile app developers see Dusty-Lee Donnelly, 'Data Privacy in the Cloud: The Position of SMMEs Engaged in Mobile App Development in South Africa' in Singh U and others (eds), *Global Trends in Management, IT and Governance in an e-World (E-MIG 2019 International)* (CSSALL Publishers 2020).

[99] Information and Privacy Commissioner Ontario Canada and Registratiekamer The Netherlands, section 1.2.

[100] The OECD Guidelines called for limits on collection while the COE Convention 108 art 5 required that data be 'adequate, relevant and not excessive', a formulation echoed in POPIA s 10 and in Directive 95/46/EC art 6(1)(a) (and now in GDPR art 5(1)(c)).

[101] See A Cavoukian and Claudiu Popa, *Privacy by ReDesign: A Practical Framework for Implementation* (Toronto, ON, Canada: Office of the Privacy Commissioner, Ontario, Canada, 2011) at 1. However, she blurs the lines of this concept by referring also to the collection of 'unnecessary data'. In data-protection laws, data minimisation is bounded by the concept of reasonableness: data can be collected only if it is reasonably necessary for a clearly specified lawful purpose.

[102] *Rīgas satiksme* (C-13/16) ECLI:EU:C:2017:336 para 38. Although the judgment was decided under Directive 95/46/EC, the remarks apply with equal force ot GDPR and POPIA.

'Another important data protection principle is "transparency" or "openness." People have the right to know what data about them have been collected, who has access to that data, and what the data are being used for. The principle of transparency simply means that people must be made aware of the conditions under which their information is being kept and used.

The principle of transparency may also be used to explain the logic behind the data processing underlying a collection — asking for identifying information in a situation that does not strictly require it, must be questioned. Indeed, the collection and use of personal data for identification purposes when not truly necessary (where alternatives are available), cannot be supported in relation to the principles noted above. Since these data protection principles are incorporated into most privacy laws such as the Ontario Freedom of Information and Protection of Privacy Act and the Dutch Privacy Act (Wet persoonsregistraties), or EU-directive SYN 287, in some situations, the unnecessary collection of identifiable data may have a direct bearing on compliance with these statutes.'[103]

The key insight was that the approach had to involve deciding from the outset of the design phase what personal data was truly necessary. Hence privacy 'by design'. The rationale for this approach is that it is required by the principles of purpose specification and use limitation.

'One of the basic principles in both the OECD guidelines and Convention 108 is the principle of "purpose specification". The quantity and nature of personal data that an organization is permitted to collect is limited by the purpose of the collection. The primary rule is that the data be relevant and sufficient, but not excessive for the stated purpose. In other words, the personal information to be collected must be needed to carry out the stated purpose.

This principle also seeks to ensure that restraint is exercised when personal data are collected. In accordance with this principle, one may question when identifying data is being sought from individuals where it is not necessary to do so. This is associated with the "use limitation principle", where the purpose specified to the data subject at the time of the collection restricts the use of the information collected. Thus, the information

[103] Information and Privacy Commissioner Ontario Canada and Registratiekamer The Netherlands section 1.2.

collected may only be used for the specified purpose (unless consent has been obtained for additional uses).'[104]

The report also emphasises consumer concern for privacy and that consumer trust is essential to widespread adoption of digital solutions, but lack of awareness reflects in low demand for the implementation of privacy measures.[105] On this basis, the report recommended that privacy regulators promote the idea that designers 'make use of privacy-enhancing technologies wherever possible'.[106] What is required is that privacy be made a default setting.[107]

Hence privacy *by default* was proposed as a necessary corollary to PbD, for if a system is designed on the basis of privacy-enhancing technologies *and* complies with the principles of data minimisation and purpose limitation, then *by default*, privacy is protected. The data subject and user of the technology is not required to be aware of and take steps to protect privacy, as the system is designed to do so.

VIII PRIVACY BY DESIGN AND THE CONCEPT OF INFORMED CONSENT

The concept of PbD, like the data protection principles, sets out abstract high-level principles, but regulators need specific guidance on expectations in the context of mobile applications,[108] and app developers need the legal requirements to be 'translated' into concrete, context-specific development goals.[109] PbD claims to have moved beyond a 'notice and consent' model, and

---

[104] Information and Privacy Commissioner Ontario Canada and Registratiekamer The Netherlands, section 1.4.

[105] ibid section 2.3. There are numerous studies reporting similar findings. See e.g. Carlos Flavián and Miguel Guinalíu, 'Consumer Trust, Perceived Security and Privacy Policy' (2006) 106 *Industrial Management & Data Systems* 601–620 and James P Lawler, 'Customer Loyalty and Privacy on the Web' (2003) 2 *Journal of Internet Commerce* 89–105.

[106] Information and Privacy Commissioner Ontario Canada and Registratiekamer The Netherlands section 3.1. The report makes it clear that data protection authorities have a key role to play as such technologies will not be widely offered without consumer demand (hence the need for intensive public awareness campaigns) or regulatory measures to enforce compliance with the statutory requirements.

[107] Information Commissioner's Office (UK), *Guide to the General Data Protection Regulation (GDPR)* (2019) at 188. European Data Protection Supervisor (EDPS), *Opinion 5/2018 Preliminary Opinion on Privacy by Design* (2018) at 7.

[108] Martin and Shilton at 201.

[109] For a pointed critique see ENISA at 47, Rubinstein and Good at 1407, and Michelle Finneran Dennedy, Jonathan Fox and Thomas R. Finneran, *The Privacy Engineer's Manifesto: Getting from Policy to Code to QA to Value* (Apress Open 2014) at 89. Also see Irit Hadar and others, 'Privacy by Designers: Software Developers' Privacy Mindset' (2018) 23 *Empirical Software Engineering* 259–289, Inah Omoronyia and others, 'Engineering Adaptive Privacy: On the Role of Privacy Awareness Requirements' in *Proceedings of the 2013 International Conference on Software Engineering* (IEEE, San Francisco CA 18–26 May 2013), Swapneel Sheth, Gail Kaiser and Walid Maalej, 'Us and Them: A Study of Privacy Requirements Across North America, Asia, and Europe'

the foundational principles do not directly refer to consent emphasising instead that privacy is 'designed' in and protected by strong 'privacy-friendly' default settings. By following a PbD approach an app developer would *first* eliminate or reduce to a minimum the collection of personal information, and only then consider relying on the user's consent for the collection or sharing of personal information, such as through user granted 'permissions'.[110] Thus app developers must be guided to view *informed* consent as a key development goal.

While consent has been strenuously criticised as inadequate,[111] others argue that the key lies in retaining consent as one justification for lawful processing, but strengthening notice (that is, transparency).[112] As the model of free services in exchange for personal information is only likely to expand,[113] the question of how purposes of processing are to be explained, and to what degree of specificity, become crucial. Furthermore, as ubiquitous third-party processing is virtually undetectable to the average user, the requirement must be on the responsible party collecting the information directly from the data subject to provide clear notice of the identity of all third parties with whom information will be shared. Restricting processing to a 'strict minimum'[114] may be impractical and have the undesired consequence of thwarting technological development and the free flow of information, contrary to the goals of data protection laws. Therefore, it is submitted that to advance the implementation of a PbD approach, a legal analysis is required of the definitions of personal information, the responsible

---

in *Proceedings of the 36th International Conference on Software Engineering* (ACM, Hyderabad, India 31 May–7 June 2014), Ira S Rubinstein, 'Regulating Privacy by Design' (2011) 26 *Berkeley Tech LJ* 1409–1546, and Keerthi Thomas and others, 'Distilling Privacy Requirements For Mobile Applications' in *Proceedings of the 36th International Conference on Software Engineering* (ACM, Hyderabad, India 31 May–7 June 2014).

[110] The concept of permissions was explained in chapter 2.

[111] Ehimare Okoyomon and others, 'On The Ridiculousness of Notice and Consent: Contradictions in App Privacy Policies' (The Workshop on Technology and Consumer Protection (ConPro '19), 2019) and Wright, 2018 #1100. Cf Daniel Susser, 'Notice After Notice-and-Consent: Why Privacy Disclosures Are Valuable Even If Consent Frameworks Aren't' (2019) 9 *Journal of Information Policy* 37–62. See further in a health data context: C. Staunton and others, 'Safeguarding the Future of Genomic Research in South Africa: Broad Consent and the Protection of Personal Information Act No. 4 of 2013' (2019) 109 *South African Medical Journal* 468–470, Farzaneh Karegar, 'Towards Improving Transparency, Intervenability, and Consent in HCI' (Karlstad University Press 2018), and Mzukisi Niven Njotini, 'Preserving the Integrity of Medical-related Information – How "Informed" is Consent?' (2018) 21 *Potchefstroom Electronic Law Journal* 1–20.

[112] International Working Group on Data Protection in Telecommunications, *Working Paper on Big Data and Privacy: Privacy principles under pressure in the age of Big Data analytics* (May 2014, Skopje, 2014) at para 18 and fn 36.

[113] Ibid.

[114] Cavoukian, 'Privacy by Design The 7 Foundational Principles Implementation and Mapping of Fair Information Practices' at 3. Here Cavoukian explains the data minimisation principle to mean 'the collection of personally identifiable information should be kept to a strict minimum'.

party, consent, notice and other grounds of lawful processing, and the principles of data minimisation and accountability as they pertain to data protection instruments.

X CONCLUSION

While PbD has been embraced by regulators as an important concept, a PbD approach needs concrete articulation in both enforceable legal obligations and defined software development goals. This chapter has demonstrated that two principles in particular thus lie at the heart of an effective PbD approach: data minimisation and accountability. A fortiori to achieve Pb(re)D in the existing, complex mobile apps ecosystem described in chapter 2, a clear understanding of the legal principles of data minisation and accountability is required. These principles will be addressed in the country-specific chapters that follow, along with the definitions in those jurisdictions of key concepts, namely: personal information, the responsible party, consent (as the primary basis for lawful processing), notice, and other grounds of lawful processing.

CHAPTER 4

US DATA PROTECTION LAW

I INTRODUCTION

At a federal level, the protection of personal information of individuals interacting with government agencies in the US is regulated principally by the Privacy Act, 1974[1] and the e-Government Act of 2002,[2] although it remains an area of considerable complexity.[3] However, as yet there is no general privacy statute which regulates private sector collection and use of personal information.[4] Instead, the US has adopted a sector-specific approach to data protection legislation, coupled with self-regulation.

---

[1] The Privacy Act of 1974, 5 U.S.C. § 552a (2018). For a criticism of its 'antiquated' provisions, see Paul M Schwartz and Daniel J Solove, 'The PII Problem: Privacy and a New Concept of Personally Identifiable Information' (2011) 86 *NYUL Rev* 1814–1894 at 1824.

[2] e-Government Act of 2002, Pub Law 107–347, 116 Stat. 2899.

[3] A vast number of statutes must be read alongside the Privacy Act of 1974 and the e-Government Act of 2002. Access to information is regulated under the The Freedom of Information Act of 1966, 5 U.S.C. § 552 (2018) (FOIA, US) (FOIA US). Government surveillance is regulated under the protection afforded against unreasonable search and seizure in the Fourth Amendment of the US Constitution. Foreign intelligence surveillance activities are regulated under the Foreign Intelligence Surveillance Act of 1978, 50 U.S.C. §§ 1801–1885c (2018) (FISA) (FISA), as amended.[3] The retention of phone call metadata by cellular network provider, and its use by government, is regulated by the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, Pub.L. 107–56, 115 Stat. 272 (USA Patriot Act), as amended by the USA Freedom Act of 2015, Pub Law No. 114-23, 129 Stat. 268 (2015). Responsibility for security of government information systems rests with federal agencies and the National Institute of Standards and Technology (NIST) who report to the Office of Management and Budget (OMB) under the Federal Information Security Modernization Act of 2014, Pub.L. No. 113–283, 128 Stat. 3073 (FISMA). The FedRAMP program established by the OMB operates to standardise the authentication of secure cloud services for use by government agencies. A full list of accredited cloud service providers and the independent accreditation agencies who vet those services can be found at 'FedRAMP' <https://www.fedramp.gov/> accessed 22 February 2020.

[4] There were calls for such legislation from the Federal Trade Commission, the US Department of Commerce and the office of the White House in 2012, but the 'Consumer Privacy Bill of Rights Act 2015 Discussion Draft' <https://obamawhitehouse.archives.gov/sites/default/files/omb/legislative/letters/cpbr-act-of-2015-discussion-draft.pdf> accessed 13 May 2020 failed to attract any support. In December 2019 the bipartisan Energy and Commerce Committee of the House of Representatives issued the US Consumer Data Privacy Act of 2019 (discussion draft) available at https://aboutblaw.com/NaZ, accessed on 25 February 2020. Several Senate bills have also been tabled, chiefly the Democrat senator Cantwell sponsored Consumer Online Privacy Rights Act, S.B. 2968, 116th Congress, 1st session (2019) (COPRA) and a draft Consumer Data Privacy Act of 2019 (CPDA), released by Republican Senator Wicker in December 2019. However, there is a slew of other senate bills including: The Customer Online Notification for Stopping Edge-provider Network Transgressions (CONSENT) Act 115 Con. 2nd session, Data Care Act of 2018 S.3744 — 115th Congress, American Data Dissemination Act of 2019 S.142 — 116th Congress (2019–2020), Social Media Privacy Protection and Consumer Rights Act of 2019 S.189 116th Congress (2019–2020), Algorithmic Accountability Act of 2019 S.1108 116th Congress (2019–2020), and Designing Accounting Safeguards To Help Broaden Oversight and Regulations on Data (DASHBOARD) Act S.1951 — 116th Congress (2019–2020). For contemporary comment, see Paul Bischoff, 'What is the Consumer Privacy Bill of Rights?' (27 November 2018) <https://www.comparitech.com/blog/vpn-

After extensive investigations, the FTC recognised that self-regulation was insufficient to ensure the protection of personal information. It recommended legislative intervention in relation to the information of children,[5] which led to the enactment of the Children's Online Privacy Protection Act (1998) (COPPA).[6] Although it initially gave qualified support for the self-regulation approach to online privacy generally,[7] from 2000 it has recommended the adoption of a federal consumer privacy statute to complement self-regulatory and education measures.[8]

Data protection is also addressed in a myriad of state laws.[9] One state in particular, however, has taken a very proactive approach to privacy. California has enacted the California Online Privacy Protection Act (2004) (CalOPPA)[10] and more recently the Consumer Privacy Protection Act (2018) (CCPA),[11] both of which regulate the collection and processing of the personal information of California residents. That approach is now being adopted by bills put forward in other states,[12] and the spectre of regulatory compliance burdens under multiple state laws has shifted industry attitudes towards support for a federal privacy bill. Several bills are presently before Congress.[13]

---

privacy/consumer-privacy-bill-of-rights/> accessed 25 February 2020, Ro Khanna, 'Rep. Khanna releases 'Internet Bill of Rights' principles, endorsed by Sir Tim Berners-Lee' (4 October 2018) <https://khanna.house.gov/media/press-releases/release-rep-khanna-releases-internet-bill-rights-principles-endorsed-sir-tim> accessed 25 February 2020 and Lourdes Turrecha, 'Americans might be getting a comprehensive federal privacy law soon' (18 February 2020) <https://medium.com/golden-data/americans-might-be-getting-a-comprehensive-federal-privacy-law-soon-64bc6e03ab94> accessed 25 February 2020.

[5] Federal Trade Commission, *Privacy Online: A Report to Congress* (1998). Its findings regarding the vast amounts of information collected online from children prompted the FTC to immediately recommend protection of children in particular. While the report (at 50) indicated that further recommendations would follow on online consumer privacy in general, a general online privacy statute has not yet been enacted in the US.

[6] Children's Online Privacy Protection Act of 1998, 15 U.S.C. §§ 6501 - 6506 (2018) (COPPA).

[7] Federal Trade Commission, *Self-regulation and Privacy Online: A Report to Congress* (July 1999).

[8] Federal Trade Commission, *Privacy Online: Fair Information Practices in the Electronic Marketplace: A Report to Congress* (May 2000). Its approach has not always been consistent but is now being joined by industry calls for such a law.

[9] See generally Schwartz and Solove.

[10] The Online Privacy Protection Act of 2003, Cal. Bus. & Prof. Code §§ 22575–22579 (2004).

[11] The California Consumer Privacy Act of 2018, Cal. Civ. Code §§ 1798.100 - 1798.199 (CCPA).

[12] An overview of state consumer privacy statutes is available at National Conference of State Legislatures (NCSL), '2019 Consumer Data Privacy Legislation' (2019) <https://www.ncsl.org/research/telecommunications-and-information-technology/consumer-data-privacy.aspx> accessed 25 February 2020.

[13] Roger Wicker, 'Chairman's Statement at US Senate Committee on Commerce, Science and Transportation Hearing: Examining Legislative Proposals to Protect Consumer Data Privacy' (4 December 2019) <https://www.commerce.senate.gov/2019/12/examining-legislative-proposals-to-protect-consumer-data-privacy> accessed 25 February 2020. Analysis of these bills is beyond the scope of this dissertation. Key sticking points are whether the federal bill would pre-empt state legislation and which federal agency would have regulatory oversight in respect of the bill.

This chapter will examine the provisions of COPPA, CalOPPA, and the CCPA in relation to key concepts, namely: personal information, the responsible party, consent (as the primary basis for lawful processing), notice, and other grounds of lawful processing. It will further consider how data minimisation and accountability are addressed under these instruments. These issues were identified in chapter 3 as being central to the analysis of a PbD approach to data protection.

II THE FEDERAL POSITION: A SECTORAL APPROACH

Without any rationalising federal statute setting out a uniform approach to defining personal information and core data protection principles, the US approach has resulted in a complex patchwork of legislative measures with overlapping but not always consistent protection measures, and a network of different enforcement agencies,[14] with the potential for some collection of personal information to fall through the proverbial cracks.

---

[14] See for example:

- Cable Communications Policy Act of 1984, 47 U.S.C. § 551 (2018) in respect of cable subscriber's information,
- Communications Act of 1934, as amended by, Telecommunications Act of 1996, 47 U.S.C. § 222 (2018) in respect of 'customer proprietary network information'(CPNI) related to telecommunications services (and the CPNI rules enacted by the Federal Communications Commission (FCC),
- Electronic Communications Privacy Act of 1986, 18 U.S.C. §§ 2510 (2018) (ECPA) in respect of interception of communications content by electronic means, updating Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (Wiretap Act) Pub. L. 90-351 34 U.S.C. §10101, and enacting Stored Communications Act (SCA) Pub.L. 99–508 100 Stat. 1848 18 U.S.C. §§ 2701–2712.
- Fair Credit Reporting Act of 1970, 15 U.S.C. § 1681 (2018) (FCRA) in respect of the accuracy, fairness and privacy of consumer information held by credit bureaus,
- Family Educational Rights and Privacy Act of 1974, 20 U.S.C. § 1232g; 34 C.F.R. §§ 99.1–99.8 (FERPA) in respect of an 'educational record' held by a school funded by the US Department of Education,
- Gramm-Leach-Bliley Act of 1999, Pub.L. No. 106–102, 113 Stat. 1338 (GLBA) in respect of data collection and sharing by a 'financial institution',
- Health Insurance Portability and Accountability Act of 1996, Pub.L. No. 104–191, 110 Stat. 1936 (HIPAA) in respect of 'personal health information' held by a 'covered entity',
- Health Information Technology for Economic and Clinical Health (HITECH) Act, Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009 (ARRA), Pub. L. No. 111-5, 123 Stat. 226 (HITECH Act)introducing civil and criminal liability for privacy and security breach by a 'business associate' suppling health IT to HIPAA-covered entities,
- Right to Financial Privacy Act of 1978, 12 U.S.C. §§ 3401 (2018) in respect of bank records,
- Telephone Consumer Protection Act of 1991 (TCPA) 47 U.S.C. § 227 and Controlling the Assault of Non-Solicited Pornography And Marketing (CAN-SPAM) Act of 2003, Pub.L. 108–187 Stat.2699 15 U.S.C. § 7701 et seq. in respect of direct marketing by telephone and email; and
- Video Privacy Protection Act of 1988, 18 U.S.C. § 2710 (2018) in respect of 'pre-recorded video cassette tapes and similar audio-visual material'.

For example, the collection and dissemination of 'personal health information' by a 'covered entity' is regulated under the Health Insurance Portability and Accountability Act (1996) (HIPAA),[15] but if a school holds medical information on a scholar in an 'educational record' it may be regulated under the Family Education Rights and Privacy Act (1974) (FERPA),[16] or under both HIPAA and FERPA. On the other hand, health information may not be protected at all if the entity collecting it or the type of data file does not fall within the scope of the federal legislation.[17] This is precisely the case with m-health apps. Developers who are HIPAA-covered entities, or business associates of such entities,[18] are liable to civil and criminal liability for failure to comply with the privacy and security safeguards required under HIPAA. However, developers of a health app that allows users to upload their own health information, or information the users have obtained from their medical advisers, will not be regulated under HIPAA.[19]

Secondly, those operations defined as 'financial institutions' dealing with a consumer's 'non-public personal information' must comply with the Gramm Leach Bliley Act (GLBA),[20] and GLBA privacy rule,[21] which they can do by adopting a model privacy notice, and a fresh notice when practices change.[22] The FTC's safeguards rule[23] continues to apply to financial institutions under its jurisdiction, and the requirement for a written security plan has been supplemented by recent proposed amendments.[24] Mobile app developers and app

---

[15] HIPAA. The Act must be read together with the regulations under the HIPAA Privacy Rule, 45 C.F.R. parts 160 & 164 (A) & (E) (2018) and HIPAA Security Rule, 45 C.F.R. parts 160 and 164 (A) & (C) (2018). See further US Department of Health and Human Services, 'Health Information Privacy' <https://www.hhs.gov/hipaa/for-professionals/privacy/index.html> accessed 21 February 2020.

[16] FERPA.

[17] See generally Paul M Schwartz, 'The EU-US Privacy Collision: A Turn to Institutions and Procedures' (2012) 126 *Harv L Rev* 1966–2009 at 1975. The author does not refer specifically to mobile applications but discusses the risk of health data being unprotected. However, Schwartz is generally opposed to an omnibus federal privacy statute. See Paul M Schwartz, 'Preemption and Privacy' (2008) 118 *Yale LJ* 902–947.

[18] Liability of business associates, such as developers of health IT products, was introduced by the HITECH Act.

[19] See guidance available on the developer's portal of the US Department of Health and Human Services, 'Health App Use Scenarios & HIPAA' (February 2016) <https://hipaaqsportal.hhs.gov/community-library/accounts/92/925889/Public/OCR-health-app-developer-scenarios-2-2016.pdf> accessed 22 February 2020.

[20] GLBA.

[21] Privacy of Consumer Financial Information (Regulation P), 12 C.F.R. part 1016 (2020). Also see FTC Privacy of Consumer Financial Information Rule, 16 C.F.R part 313 (2019).

[22] The amendment of the requirement to give annual notice was effected in the Fixing America's Surface Transportation (FAST) Act of 2015, Pub. L. No. 114-94 (FAST Act), title LXXV-Eliminate privacy notice confusion, amending s 503 of the GLBA.

[23] Standards for Safeguarding Customer Information, 16 C.F.R. § 314.

[24] Privacy of Consumer Financial Information Rule Under the Gramm-Leach-Bliley Act: A Proposed Rule by the Federal Trade Commission, 84 FR 13150 (22 February 2020). This proposed amendment would require financial

providers developing mobile apps constituting 'financial services' are thus subject to oversight from multiple agencies.

Thirdly, US eavesdropping legislation[25] protects communications content, not 'record data', such as logs generated automatically about the origin, time and duration of the communication (that is, metadata).[26] Even if metadata may be 'personally identifiable information', it is not covered under this legislation,[27] unless it reveals the contents of a communication.[28] The line between content and record is thus 'relative'[29] rather than being fixed by the type of data in question or whether data can be linked to a particular individual or device.[30]

---

institutions to encrypt, inter alia, all customer data at rest or transmitted over external networks and institute multifactor authentication for account access, or similar measures (and conduct regular threat monitoring and testing) under the oversight of a dedicated chief information security officer.

[25] In the US, this is the ECPA, which amends the Wiretap Act. For the position in the EU and South Africa, see chapters 5 and 6.

[26] *In re Zynga Privacy Litigation* 750 F3d 1098, 1105-06 (9th Cir 2014) at 1106. Under the Wiretap Act, as amended by ECTA, 18 U.S.C. § 2510(12), an electronic communication is broadly defined as 'any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electro-magnetic, photoelectric, or photooptical system that affects interstate or foreign commerce'. The Act permits a private right of action against any person who 'intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication' (18 U.S.C. § 2511(1)(a) read with 18 U.S.C. § 2520). However, the scope of this right is limited as *an interception* is defined as 'the aural or other acquisition of the *contents* of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device' (own emphasis). 'Contents,' is defined to 'include any information concerning the substance, purport, or meaning of that communication'.

[27] *In re Zynga Privacy Litigation* at 1107. Cf *In re Pharmatrak* 329 F3d 9, 15, 18–19 (1st Cir2003) which held that 'content' must be broadly interpreted and includes 'personally identifiable information such as a party's name, date of birth, and medical condition'. The case is distinguishable on the facts from *In re Zynga Privacy Litigation* as Pharmatrak did not deny the interception element. In any event the information appeared in forms actually filled out by users on the websites of pharmaceutical companies. See further, cited in support, *Gelbard v United States* 408 US 41 (1972) at 51, that '[n]o aspect, including the identity of the parties … is excluded. The privacy of the communication to be protected is intended to be comprehensive'. However *Gelbard* refers to the original definition of 'content' in the Wiretap Act 18 U.S.C. § 2510(8), which expressly included both the 'identity of the parties' and the 'existence' of the communication. Section 101(a)(5) of ECPA amended the definition by striking out those words. This is not referred to in *In re Pharmatrak.*

[28] *In re Google Inc. Cookie Placement Consumer Privacy Litigation* 806 F3d 125 (3d Cir 2015) at 138, finding that a queried URL (which could include search terms communicated to a search engine, or otherwise detail the content being requested) could be content as well as traffic data (a routing instruction to the web browser). See further Orin S. Kerr, 'Applying the Fourth Amendment to the Internet: A General Approach' (2010) 62 *Stan L Rev* 1005–1049 at 1030.

[29] *In re Google Inc. Cookie Placement Consumer Privacy Litigation*.

[30] The claim did not make out a cause of action under the Wiretap Act on the grounds that Google were a party to the communication (not an interceptor), as the plaintiffs' browsers would communicate directly to the defendants' servers to request delivery of advertising content. However, Google were in fact placing a third-party cookie on the browser to facilitate targeted advertising, by-passing 'cookie blockers' set by default in the Apple Safari browser, or set by users in Windows Explorer, and contrary to its own privacy disclosures. See Jonathan Mayer, 'Safari Trackers' (17 February 2012) <http://webpolicy.org/2012/02/17/safari-trackers/> accessed 26 February 2020. It was held that notwithstanding possible fraud or deceit by Google, the plaintiff's case did not make out a

This creates a problem in the mobile apps ecosystem since apps can run in the background collecting data without the user's knowledge and consent while the user is not even on their device. The existing US case law has been unable to accommodate this data transfer within the concept of a user 'communication'. Thus federal law[31] has been held inapplicable to location data and device IDs collected by the ad network Kiip from mobile apps,[32] and the Facebook IDs[33] and browser referrer URLs[34] collected from Facebook users by the Zynga app and shared with advertisers.[35]

From 1995 the Federal Trade Commission (FTC) has taken an active role in educating the public and industry about online privacy.[36] It is empowered under section 5 of the Federal Trade Commission Act (1914) (FTCA)[37] to act against unfair and deceptive trade practices. It has used these powers to seek relief against companies that do not comply with their stated privacy policies and practices.[38] However, it cannot compel any company to adopt FIPPs principles, save in respect of services directed at children.[39] Thus a federal privacy law appears necessary to implement data protection in the US effectively, but as a final bill is not yet in sight, the current laws are examined in this dissertation.

---

cause of action on any of the statutory grounds pleaded but might be actionable as an invasion of the right to privacy afforded by the California Constitution. In 2019 a $5.5 million settlement of the suit was remanded to the District Court to consider whether there was not an inappropriate significant association between Google and the proposed cy-près recipients of the settlement: *In re Google Inc. Cookie Placement Consumer Privacy Litigation* No 17-1480 (3d Cir opinion 6 August 2019). Google have already paid a $22.5 million civil penalty to settle an FTC action (without admission of liability) [*In the matter of Google Inc.* FTC Dkt No C-4336 (Oct 13, 2011) (consent order)] and a further $17 million to settle actions by several States' Attorney-General.

[31] ECPA and Wiretap Act.

[32] *Vasil v Kiip Inc.* No 16-CV-09937 (ND Ill Mar 5, 2018).

[33] When users create a Facebook profile, they must supply their real name and email address, but Facebook assigns them a 'Facebook ID', which is a number that the user can replace with their real name or an alias. See *In re Zynga Privacy Litigation*.

[34] URLs (Uniform Resource Locators) are 'unique addresses indicating the location of specific documents on the Web. The webpage a user viewed immediately prior to visiting a particular website is known as the referrer URL.' See *In re Pharmatrak*.

[35] *In re Zynga Privacy Litigation*. The Facebook ID and the web address (referrer URL) that the user was on when she clicked a link to play a Zynga app were transmitted by Zynga to advertisers. The court found that like a name and return address on mail, this was record data and not communications content.

[36] See further Federal Trade Commission, *Privacy Online: A Report to Congress*.

[37] Federal Trade Commission Act of 1914, 15 U.S.C. §§ 41 - 58 (2018) (FTCA).

[38] Federal Trade Commission, *Self-regulation and Privacy Online: A Report to Congress* at 34. See *FTC v ReverseAuction.com Inc.* Case No 00-0032 (DDC Jan 6, 2000) (consent order) (re 'spam' using email addresses obtained from a competitor website); *Liberty Financial Companies Inc.* FTC Dkt No C-3891 (Aug 12, 1999) (re: a false privacy promise to keep information anonymous) and *GeoCities* FTC Dkt No C-3849 (Feb 12, 1999) (consent order) (re: misrepresentation about the purposes for which personal information was collected from children and adults).

[39] Federal Trade Commission, *Self-regulation and Privacy Online: A Report to Congress*.

III FAIR INFORMATION PRACTICE PRINCIPLES (FIPPs)

The origin of the term 'fair information practice principles' (FIPPs)[40] is generally traced to a 1973 US Department of Health, Education and Welfare (HEW) report on information matching of computer records.[41] This report called for a federal code of 'fair information practice' resting on notice, consent, access (to correct or amend inaccurate personal information) and security measures to prevent misuse of personal information.[42] The FIPPs are also generally regarded as the basis for the OECD Privacy Guidelines,[43] which, as described earlier, articulated a set of eight data protection principles that have been hugely influential upon regional and national data protection frameworks. The US is a member of the OECD,[44] and participates in the APEC Privacy Framework.[45] The FIPPs have thus shaped the American approach to data protection.[46] However, this is not to say that all eight data protection principles outlined in the OECD

---

[40] The term fair information principles (FIPs) is also frequently used in discussion of data protection, but the term FIPPs is used in this dissertation to avoid confusion with the National Institute of Standards and Technology (NIST) Federal Information Processing Standards. NIST, 'FIPS' <https://csrc.nist.gov/publications/fips> accessed 26 October 2019.

[41] US Department of Health Education and Welfare, *Records, Computers and the Rights of Citizens* (1973). Data protection laws already existed in certain countries in Europe. For a full discussion of the history of early data protection laws see David H. Flaherty, *Protecting Privacy in Surveillance Societies: The Federal Republic of Germany, Sweden, France, Canada, and the United States* (The University of North Carolina Press 1989).

[42] US Department of Health Education and Welfare at xx-xxi. The five principles are articulated in the report as follows:

'• There must be no personal data record-keeping systems whose very existence is secret.
• There must be a way for an individual to find out what information about him is in a record and how it is used.
• There must be a way for an individual to prevent information about him that was obtained for one purpose from being used or made available for other purposes without his consent.
• There must be a way for an individual to correct or amend a record of identifiable information about him.
• Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take precautions to prevent misuse of the data.'

[43] OECD, *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980), which were updated in 2013: OECD, *Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data* (C(80)58/FINAL, as amended on 11 July 2013 by C(2013)79, 2013).

[44] OECD, 'List of OECD Member countries - Ratification of the Convention on the OECD' <https://www.oecd.org/about/document/list-oecd-member-countries.htm> accessed 26 Oct 2019.

[45] APEC, *APEC Privacy Framework (2015)* (APEC#217-CT-019, 2017), updated from the 2005 APEC, *APEC Privacy Framework* (APEC#205-SO-012, 2005). There are 21 member economies of APEC including the US. APEC, 'List of APEC member states' <https://www.apec.org/About-Us/About-APEC/Member-Economies.aspx> accessed 26 October 2019.

[46] For fuller discussion of US policy and legislation see Priscilla M. Regan, *Legislating Privacy: Technology, Social Values, and Public Policy* (2 edn, University of North Carolina Press 1995).

Guidelines have been uniformly adopted. There have often been crucial differences in the content of FIPPs expressed in data protection laws (both within and outside the US).[47]

In 2000, the US Federal Trade Commission (FTC) published its Fair Information Practice Principles (FIPPs) incorporating only four FIPPS: notice, choice (consent), access and security.[48] These FIPPs were preceded by earlier iterations of notice and consent[49] as key elements for regulating data protection in electronic information technology (IT) systems.[50] The approach is one of modified contractual consent, where regulation imposes a notice obligation on service providers on the premise that this will permit consumers to make an informed choice about whether or not to use the service (and implicitly consent to data collection).[51]

In line with the doctrine of freedom of contract, a fundamental feature of the US approach is that collection and use of personal information is permissible unless it is prohibited by a statute.[52] Whereas EU and South African law both include a requirement that processing

---

[47] See the discussion in Paul M Schwartz, 'Beyond Lessig's Code for Internet Privacy: Cyberspace Filters, Privacy Control, and Fair Information Practices' [2000] *Wis L Rev* 743–788 at 779, and Schwartz, 'Preemption and Privacy'.

[48] Federal Trade Commission, *Privacy Online: Fair Information Practices in the Electronic Marketplace: A Report to Congress*.

[49] See the collection principle articulated in US Govt. Information Infrastructure Task Force (IITF) Privacy Working Group, *Privacy and the National Information Infrastructure: Principles for Providing and Using Personal Information* (6 June 1995) (IITF *Privacy Principles*). Also see National Telecommunications and Information Administration (NTIA) and US Department of Commerce, *Privacy and the NII: Safeguarding Telecommunications-Related Personal Information* (Washington DC) and US White House Office, *The Framework for Global Electronic Commerce* (1997).

[50] Sight should not be lost of the fact that the IITF *Privacy Principles* (which were intended to apply to government and the private sector) set out an overarching 'information privacy principle': 'Personal information should be acquired, disclosed, and used only in ways that respect an individual's privacy'. Further, they provided:

'III. Principles for Information Users (i.e. Information Collectors and entities that obtain, process, send or store personal information)

A. Acquisition and Use Principles

Users of personal information must recognize and respect the stake individuals have in the use of personal information. Therefore, users of personal information should:

1. Assess the impact on personal privacy of current or planned activities before obtaining or using personal information;

2. *Obtain and keep only information that could reasonably be expected to support current or planned activities and use the information only for those or compatible purposes*;

3. Assure that personal information is as accurate, timely, complete and relevant as necessary for the intended use;' (own emphasis).

[51] National Telecommunications and Information Administration (NTIA) and US Department of Commerce at part III.

[52] Schwartz, 'The EU-US Privacy Collision: A Turn to Institutions and Procedures'.

may not take place without a lawful basis,[53] there is no such general statutory prohibition in the US.[54] There is also no right to privacy in the US Constitution.[55] The constitutional protection of privacy under the prohibition against unreasonable search and seizure does not extend to information that has been voluntarily disclosed to a third party.[56] Further, the first amendment right to free speech would apply when the collection and dissemination of personal information falls under the protection of 'commercial speech'.[57] Hence, processing that falls outside the scope of prohibitions contained in sector-specific US legislation is prima facie lawful. Moreover, US law is generally in favour of self-regulation of the internet,[58] and fearful that over-broad government regulation may stifle innovation and profits.[59]

Bearing in mind these important substantive differences in approach, caution should be exercised in relying on the broad generalisation that core data protection principles

---

[53] The responsible party/data controller must prove that collection was lawful based either on consent, or some other lawful ground such as legitimate interests of the responsible party/data controller.

[54] Schwartz, 'The EU-US Privacy Collision: A Turn to Institutions and Procedures'.

[55] By contrast the State of California introduced a right to privacy into the Constitution of California in 1974. California Constitution. Article 1 (adopted in 1879) was amended to add section 1, on 5 November 1974 by Proposition 7. Resolution Chapter 90, 1974. Section 1 reads:
'All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, *and privacy*' (own emphasis).
The right of access to information (s 3(b)(1)) is subordinated to the right to privacy (in terms of s 3(b)(3)).

[56] Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for businesses and policymakers* (March 2012) at 62. *United States v Miller* 425 US 435 (1976) and the third party doctrine will be discussed later.

[57] 'Commercial speech' is speech or writing in which a business entity proposes a transaction to a customer. *Central Hudson Gas & Electric Corp. v Public Service Commission* 447 US 557 (1980) at 567. The sale of personal information by a credit bureau has been recognised as commercial speech. See *Dun & Bradstreet Inc. v Greenmoss Builders Inc.* 472 US 749 (1985). Also see Federal Trade Commission, *Privacy Online: Fair Information Practices in the Electronic Marketplace: A Report to Congress*: Dissenting Opinion of Commissioner Orson Swindle at 24.

[58] This approach adopted in 1997 when the World Wide Web was still in its infancy (Tim Berners-Lee had publically announced the WWW project on 6 August 1991) remains the approach taken today. See US White House Office and US White House Office, *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy* (February 2012). Both reports favour minimal regulation to avoid stifling innovation, although the 2012 report unveiled modest plans for a 'consumer privacy bill of rights' that would enshrine the 'respect for context' and 'reasonable collection limitation' principles outlined in a Federal Trade Commission Privacy Framework: Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for businesses and policymakers*.

[59] *Central Hudson Gas & Electric Corp. v Public Service Commission* supra note 57 developed a four-part test for government regulation of 'commercial speech':

1. Whether the commercial speech concerns a lawful activity and is not misleading
2. Whether the government interest asserted to justify the regulation is "substantial"
3. Whether the regulation "directly advances" that government interest
4. Whether the regulation is no more extensive than necessary to serve that interest.

are 'broadly similar'.[60] The specific terms in which data protection principles are protected in COPPA, CalOPPA and the CCPA will now be considered.

IV THE CHILDREN'S ONLINE PRIVACY PROTECTION ACT (1998) (COPPA)

(a) Origin and background

The COPPA Rule[61] was issued by the FTC pursuant to its regulatory powers under COPPA and came into force on 21 April 2000. The Rule regulates the activities of 'operators of web sites or online services directed to children' under 13,[62] or where the operator of the website or online service has 'actual knowledge that they are collecting personal information online from a child'.[63] Principally, the COPPA Rule requires that operators provide parents with 'notice'[64] and 'obtain verifiable parental consent prior to collecting, using, or disclosing personal information obtained from children'.[65] The COPPA Rule also limits collection by controlling 'conditioning'[66] of children through prizes or other incentives to provide unnecessary personal information, and requires reasonable security measures to be taken to safeguard the personal information of children.

Pursuant to the FTC review commenced in 2010, the COPPA Rule was amended with effect from 1 July 2013. The key amendments relevant to this study are the expanded definition of 'personal information' (to cover linking of information to an individual via online identifiers) and the revised definition of 'operator' (to cover operators who integrate third party

---

[60] Anneliese Roos, 'The law of data (privacy) protection: a comparative and theoretical study' (2009) at 22, citing Colin J. Bennet, *Regulating privacy : data protection and public policy in Europe and the United States* (Cornell University Press 1992). The greatest differences between the US and EU approach remain procedural. Namely, the choice of sectoral regulation in the US versus an 'omnibus' statute in the EU, and the EU approach of establishing a central data protection office in each member country and an EU supervisory body under the Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA OJ L 119, 4.5.2016 (EU General Data Protection Regulation; GDPR).

[61] Children's Online Privacy Protection Rule, 16 C.F.R part 312 (COPPA Rule).

[62] COPPA Rule §312.3. A 'child' is defined as 'an individual under the age of 13'. 15 U.S.C. §6501(1) and COPPA §312.2.

[63] Ibid.

[64] COPPA Rule § 312.2(a) requires notice of what information is collected from the child, and how it is used and to whom it is disclosed, as further regulated by § 312.4 (discussed below).

[65] COPPA Rule § 312.3(b), as further regulated by § 312.5 (discussed below).

[66] The term used in COPPA Rule § 312.3(d) and § 312.7 is not further defined.

services such as plugins or ad networks). Further amendments may be effected after the conclusion of the review initiated in 2019.[67]

(b) Personal Information

Under COPPA the term 'personal information' means 'individually identifiable information about an individual collected online'.[68] The term is broadly defined. It expressly includes 'first and last name', 'home or other physical address including street name and name of a city or town', 'an e-mail address', 'a telephone number' and 'a Social Security number'.

However, it also includes certain online identifiers[69] and any information concerning a child or his or her parents that is collected online from the child and combined with such identifier.[70] Under the COPPA Rule, an online identifier would include 'online contact information'[71] such as IM,[72] VOIP[73] and video chat[74] identifiers. Personal information can also comprise 'a screen or user name' used for direct messaging.[75] For example, a Twitter handle, or a gamer's 'nickname' where the game enables direct private messaging, can be used by another user to contact the child directly and would be personal information. The FTC

---

[67] Request for Public Comment on the Federal Trade Commission's Implementation of the Children's Online Privacy Protection Rule, FR 84(143) (25 July 2019).

[68] 15 U.S.C. §6501(8). Neither COPPA nor the COPPA Rule define an additional category of 'special' or 'sensitive' information. By virtue of its special legislative treatment all information about children is sensitive and requires special precautions for its collection, use and disclosure.

[69] 15 U.S.C. §6501(8)(F) refers to 'any other identifier that the Commission determines permits the physical or online contacting of a specific individual'.

[70] 15 U.S.C. §6501(8)(G) refers to 'information concerning the child or the parents of that child that the website collects online from the child and combines with an identifier described in this paragraph'. The definition appears ambiguous about whether information on a child collected online from another child (e.g. via a social networking platform), or from the child's parents, or collected offline or from third party sources is covered.

[71] COPPA Rule 16 C.F.R §312.2: *'Online contact information* means an email address or any other substantially similar identifier that permits direct contact with a person online, including but not limited to, an instant messaging user identifier, a voice over internet protocol (VOIP) identifier, or a video chat user identifier.' For somewhat unconvincing reasons the FTC decided not to include mobile telephones. Thus the direct notice to parents under §312.4(c) may not be sent by SMS but can be sent via another online contact medium such as email. See Children's Online Privacy Protection Rule; Final Rule Amendments, FR 79(12) Part II (17 January 2013) at 3975.

[72] IM (instant messaging) is enabled by applications such as Facebook messenger.

[73] VOIP (voice over internet protocol) enables calls over an internet connect and not a traditional telephone cable e.g. Skype.

[74] E.g. video chats are possible in Skype, Facebook Messenger, and Apple's FaceTime but there is a proliferation of other mobile apps with video chat functionality. This was largely made possible by Google's open-source WebRTC code, with libraries for integration into iOS and Android apps. 'WebRTC' <https://webrtc.org/> accessed 4 March 2020.

[75] COPPA Rule 16 C.F.R §312 – includes a screen name and user name as personal information under the proviso that 'it functions in the same manner as online contact information'.

regards the definition as applying to 'direct, private, user-to-user contact'.[76] Thus operators are permitted to use anonymous screen and user names (ones that do not directly identify the user by real name) without prior notice and parental consent in other cases,[77] such as for personalising content,[78] filtered[79] or moderated chat,[80] public display (for example, a screen name or user name may be displayed in a chat room or for attribution of high scores in multi-player games), operator-to-user communication, and single sign-on.[81]

In certain circumstances, personal information will also include a 'persistent identifier'.[82] COPPA defines personal information as including 'any other identifier that the Commission determines permits the *physical or online contacting of a specific individual*'[83] (own emphasis). Thus although persistent identifiers can identify a device, unless they can also make an individual 'contactable', they are not supplying personal information. The COPPA Rule, as amended in 2013, now defines personal information as including '[a] persistent identifier that can be used to recognize a user over time and across different Web sites or online services'.[84] The FTC has expressed the view that (without notice and prior parental consent) a persistent identifier cannot be 'used or disclosed to contact a specific individual, including

[76] Children's Online Privacy Protection Rule; Final Rule Amendments, FR 79(12) Part II (17 January 2013) at 3979.
[77] Ibid.
[78] A simple form of personalisation may be to include the user's screen name or user name in a greeting. The kinds of personalisation discussed in chapter 2 used by apps to recommend content and events (both in-app, and by push notifications and email) would require prior notice and consent for the collection of the other kinds of personal information used in those algorithms (e.g. location to match users to local events, and listening/viewing/browsing history to match users to interests).
[79] A chat filter automatically screens posts to a chat room for personal information and inappropriate content such as vulgar language. The COPPA Rule amendment to remove the requirement to delete 100% of personal information from children's public posts and replace it with a requirement to exercise 'reasonable measures' to remove 'all or virtually all' such personal information, reflects industry lobbying for the use of automatic filtering. See Children's Online Privacy Protection Rule; Final Rule Amendments, FR 79(12) Part II (17 January 2013) at 3973–3974.
[80] In an interactive online forum, such as a 'user community' in a gaming app, user questions and comments are first checked by the moderator for adherence to forum rules before being posted in the chatroom.
[81] Where a username and password can be used for a single account across multiple devices and platforms.
[82] COPPA Rule 16 C.F.R §312.2 provides in the definition of 'personal information' that 'such identifier includes, but is not limited to, a customer number held in a cookie, an Internet Protocol (IP) address, a processor or device serial number, or unique device identifier'. As this is not a closed list, arguably a 'semi-persistent' identifier such as a resettable advertising ID is covered when it is de facto used to track users over time.
[83] COPPA 15 U.S.C. §6501(8)(F).
[84] COPPA Rule 16 C.F.R §312.2.

through the use of behavioural advertising',[85] but may be used for 'internal services', including delivery of contextual advertising. [86]

Furthermore, the definition of personal information under the COPPA Rule now also includes photographs, video and audio,[87] and precise geo-location information.[88]

(c) Operator

The COPPA Rule applies to the 'operator'[89] of a commercial website or online service directed at children where information on the users or visitors the website or service is 'collected'[90] or 'maintained'[91] by the operator, or on the operator's behalf.

---

[85] Children's Online Privacy Protection Rule; Final Rule Amendments, FR 79(12) Part II (17 January 2013) at 3979.

[86] Ibid.

The COPPA Rule leaves open to doubt whether an advertising ID is regarded as personal information.

[87] COPPA Rule 16 C.F.R §312. I.e. photographs, video files or audio files where the child's image is visible, or the child's voice can be heard.

[88] Ibid. The definition only refers to '[g]eolocation information sufficient to identify street name and name of a city or town.' Thus a coarse-grained (approximate) location that identifies only the suburb or city (e.g. by ZIP/post code) but not a street name has not been included. The amendment solidifies the FTC's previous policy stance that such location information was personal information. Children's Online Privacy Protection Rule; Final Rule Amendments, FR 79(12) Part II (17 January 2013) at 3998.

[89] COPPA Rule 16 C.F.R §312.2 ' *Operator* means any person who operates a Web site located on the Internet or an online service and who collects or maintains personal information from or about the users of or visitors to such Web site or online service, or on whose behalf such information is collected or maintained, or offers products or services for sale through that Web site or online service, where such Web site or online service is operated for commercial purposes involving commerce among the several States or with 1 or more foreign nations; in any territory of the US or in the District of Columbia, or between any such territory and another such territory or any State or foreign nation; or between the District of Columbia and any State, territory, or foreign nation. This definition does not include any nonprofit entity that would otherwise be exempt from coverage under Section 5 of the Federal Trade Commission Act (15 U.S.C. 45)'.

[90] Ibid. '*Collects* or *collection* means the gathering of any personal information from a child by any means, including but not limited to:

(1) Requesting, prompting, or encouraging a child to submit personal information online;
(2) Enabling a child to make personal information publicly available in identifiable form. An operator shall not be considered to have collected personal information under this paragraph if it takes reasonable measures to delete all or virtually all personal information from a child's postings before they are made public and also to delete such information from its records; or
(3) Passive tracking of a child online.'

[91] The term is not defined. The COPPA Rule contains provisions on 'internal operations' such as site maintenance, as well as security and integrity of information (16 CFR §312.8) and parental rights to review information, withdraw consent and require deletion of information held (16 CFR §312.6). It is submitted that this would all be classed as maintaining information.

A mobile application is an online service[92] that is operated for commerce,[93] even if it is free to download. An app is 'directed at children' if the app (or any part of the app) targets children, which could be determined by considering a range of factors such as use of animated characters, celebrities and content that would appeal to children, or through empirical evidence of 'audience' statistics.[94] This also includes apps which are not ostensibly directed at children, but which do collect information from *users of other apps* (or websites and online services) that are directed at children.[95] Before collecting any information, apps which fall within the broad scope of the COPPA Rule (even if their primary audience is not children) must still obtain age information and obtain verified parental consent if a user self-identifies as being under 13.[96] Apps which direct users to other apps (or websites and online services) that are directed at children do not fall within the scope of the COPPA Rule for that reason alone.[97] Even when apps are not ostensibly directed at children, if the operator has 'actual knowledge' that the app is collecting information from children, it is unlawful to do so without obtaining verified parental consent.[98]

---

[92] Apps send and receive information over the internet and thus fall under COPPA as they are an 'online service'. Although the term online service is not defined in COPPA see *United States v. W3 Innovations LLC* Case No CV–11–03958 (ND Cal Aug 12, 2011)) (complaint para 12, concerning the 'Emily's World' suite of apps). Numerous cases against app developers under COPPA (discussed below) have since followed.

[93] As defined in Section 4 of the FTCA 15 U.S.C. § 44.

[94] COPPA Rule 16 C.F.R §312.2 '*Web site or online service directed to children* means a commercial Web site or online service, or portion thereof, that is targeted to children.
(1) In determining whether a Web site or online service, or a portion thereof, is directed to children, the Commission will consider its subject matter, visual content, use of animated characters or child-oriented activities and incentives, music or other audio content, age of models, presence of child celebrities or celebrities who appeal to children, language or other characteristics of the Web site or online service, as well as whether advertising promoting or appearing on the Web site or online service is directed to children. The Commission will also consider competent and reliable empirical evidence regarding audience composition, and evidence regarding the intended audience. …'.

[95] Ibid. '*Web site or online service directed to children* … (2) A Web site or online service shall be deemed directed to children when it has actual knowledge that it is collecting personal information directly from users of another Web site or online service directed to children'.

[96] Ibid. A '*Web site or online service directed to children* … (3) A Web site or online service that is directed to children under the criteria set forth in paragraph (1) of this definition, but that does not target children as its primary audience, shall not be deemed directed to children if it:
(i) Does not collect personal information from any visitor prior to collecting age information; and
(ii) Prevents the collection, use, or disclosure of personal information from visitors who identify themselves as under age 13 without first complying with the notice and parental consent provisions of this part'.

[97] Ibid. '*Web site or online service directed to children* … (4) A Web site or online service shall not be deemed directed to children solely because it refers or links to a commercial Web site or online service directed to children by using information location tools, including a directory, index, reference, pointer, or hypertext link'.

[98] COPPA §6502. Also see COPPA Rule 16 CFR §312.3. 'It shall be unlawful for any operator of a Web site or online service directed to children, or any operator that has actual knowledge that it is collecting or maintaining personal information from a child, to collect personal information from a child in a manner that violates [the COPPA Rule]'.

The 'operator' of a mobile app would be the app developer (or the app owner if the development has been outsourced). The developer will be liable under COPPA as an 'operator', whether it collects and maintains information directly, or such information is collected or maintained on its behalf.

US District Courts will assume jurisdiction under COPPA on the basis that commerce is being undertaken in the US or its territories.[99] Thus operators domiciled outside the US are subject to COPPA insofar as their online service is directed at children in the US, or they knowingly collect personal information from such children.[100] This could therefore include South African app developers if their app is downloaded by children in the US. Operators domiciled in the US must comply with COPPA (even when they are collecting information from children outside the US).[101] The FTC has also proceeded against individual officers of corporations[102] and US subsidiaries[103] on the basis that they are jointly and severally liable for the COPPA violations and resultant civil penalties and injunctive relief.

In 2015 the FTC took action against two app developers, LAI Systems[104] and Retro Dreamer,[105] for allowing third-party ad networks to collect persistent identifiers (defined as personal information since 1 July 2013) from apps directed at children for the purpose of

---

[99] District Courts Jurisdiction, 28 U.S.C. §§ 1330–1369 (2018) §§ 1331, 1337(a), 1345 and 1355, read with FTCA §§ 45(m)(1)(A), 53(b), 56(a), and 57b.

[100] E.g. the developer of TikTok was Musical.ly, a Cayman Islands registered corporation, which was subsequently acquired by Byte Dance Ltd of Beijing. *United States of America v Musical.ly* Case No 2:19-cv-01439 (CD Cal Feb 27, 2019) (proposed consent order).

[101] Federal Trade Commission, 'Complying with COPPA: Frequently Asked Questions' <https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions> accessed 8 March 2020 states:

'The Internet is a global medium. Do websites and online services developed and run abroad have to comply with the Rule?

Foreign-based websites and online services must comply with COPPA if they are directed to children in the United States, or if they knowingly collect personal information from children in the U.S. The law's definition of "operator" includes foreign-based websites and online services that are involved in commerce in the United States or its territories. As a related matter, U.S.-based sites and services that collect information from foreign children also are subject to COPPA'.

However, in practice, this has not been implemented by the TikTok app, as explained below.

[102] See e.g. *United States of America v Unixiz Inc and others* Case No 5:19-cv-2222 (ND Cal Apr 24, 2019), and *United States v Retro Dreamer and Craig E. Sharpe and Gavin S. Bowman* Case No 5:15-cv-02569 (CD Cal Dec 17, 2015).

[103] TikTok Inc, 'Privacy Policy for Younger Users' (January 2020) <https://www.tiktok.com/legal/privacy-policy-for-younger-users?lang=en> accessed 6 March 2020. TikTok Inc., a California-based corporation, published this "Privacy Policy for Younger Users" in January 2020 following the FTC action for COPPA violations by the TikTok app in *United States of America v Musical.ly*. However, this privacy policy expressly states that it applies only to children in the US.

[104] *United States v LAI Systems LLC* Case No 2:15-cv-09691 (CD Cal Dec 17, 2015).

[105] *United States v Retro Dreamer and Craig E. Sharpe and Gavin S. Bowman*.

serving in-app targeted advertising based on users' activity over time and across sites. Neither developer informed the ad networks that its apps were directed at children, nor did they notify parents and obtain verified parental consent for the collection, use and disclosure of the personal information. Retro Dreamer was informed by one ad network in 2013 that it would not continue serving ads to its apps as it believed they were directed at children. Despite this red flag, Retro Dreamer continued to allow other ad networks to collect persistent identifiers and serve targeted advertising in its apps.[106]

(d) Data Protection Principles

COPPA and the COPPA Rule do not reference the data protection principles set out in the OECD Guidelines or similar international instruments, although their requirements are in line with most of these principles. Compliance with the COPPA Rule requires an operator of a mobile app to take the following steps before it collects, uses or discloses any personal information from users:

1. Post a privacy policy on its website and in the app, setting out in clearly and understandably the disclosures required by COPPA, including what personal information is collected and how it is used and disclosed.
2. Send the disclosure notice directly to parents of the child.
3. Obtain verifiable parental consent prior to processing any personal information;
4. Inform parents that they may consent to collection and use for internal purposes and refuse consent for disclosure to third parties.
5. Provide parents access to the information collected and a means to withdraw consent for future processing and require deletion of the personal information.
6. Not 'condition' children (through incentives such as game prizes or currency) to disclose personal information that is not reasonably necessary for the activity.
7. Ensure the confidentiality, security and integrity of the information.

The report to Congress which led to the enactment of COPPA is anchored in the FIPPS articulated by the FTC: notice, consent, access, security and enforcement. Notice is 'fundamental' to the US data protection regime as it underpins the exercise of *informed* choice

[106] Both were fined, required to delete data collected from children and subjected to annual compliance reporting and record keeping of COPPA compliance activities for 10 years. No action was taken against the ad networks.

(consent).[107] Collection limitation is a 'substantive principle', in that it 'impose[s] substantive limitations on the collection and use of personal information, regardless of consumer consent, by requiring that only certain information be collected and that such information only be used in certain ways'.[108] By contrast, 'procedural principles', such as notice and consent, 'address how personal information is collected and used by governing the methods by which data collectors and data providers interact'.[109] However, notice and consent place a heavy responsibility on data subjects to read lengthy (and often ambiguous or technical) privacy disclosures, which may weaken data privacy laws and allow surveillance technologies companies to escape legal accountability.[110]

Although the report notes that the collection limitation principle requires 'that entities should only collect personal information necessary for a legitimate business purpose',[111] the principle is not discussed in its report, or expressly included in COPPA. To a limited extent, it is given effect by the COPPA Rule against 'conditioning' children through prizes or other incentives to provide more personal information than is 'reasonably necessary to participate in [the] activity'.[112] However, this provision does not regulate the automated collection of data that mobile apps facilitate. Where the 2013 amendments have significantly strengthened COPPA is in relation to accountability.

(e) Accountability

The operator is accountable for the collection and maintenance of information without verifiable parental consent and reasonable security measures, even where that collection and

---

[107] Federal Trade Commission, *Privacy Online: A Report to Congress* at 7.
[108] Ibid (at 49 note 28).
[109] Ibid.
[110] Electronic Privacy Information Centre (EPIC), *Privacy Guidelines for the National Information Infrastructure: A Review of the Proposed Principles of the Privacy Working Group* (Report 94-1, 1995).
[111] Federal Trade Commission, *Privacy Online: A Report to Congress* (at 49 note 28). By contrast collection limitation is enshrined in the Privacy Act of 1974 and requires federal agencies to collect only information that is 'relevant and necessary to accomplish a lawful purpose'. The Privacy Act of 1974, 5 U.S.C. § 552a (2018)(e)(1). See further the discussion in Privacy Protection Study Commission, *Personal Privacy in an Information Society* (US Govt Printing Office, Washington, 1977) at 513–515, which recommends that the privacy statement that must be given to the individual under 5 U.S.C § 552(a)(e)(3) should 'describe those uses of information that could reasonably be expected to influence an individual's decision to provide or not to provide the information requested' and 'should also include a description of the scope, techniques, and sources to be used to verify or collect additional information about him' (i.e. where information is collected from third parties or public sources and combined with information requested from the individual this must be disclosed). Also see IITF *Privacy Principles*.
[112]16 CRF §312.7.

maintenance is undertaken on its behalf by its service providers and agents. The COPPA Rule has always relied on consent as a key safeguard.

> *'§312.5 Parental consent.*
>
> *(a) General requirements. (1) An operator is required to obtain verifiable parental consent before any collection, use, or disclosure of personal information from children, including consent to any material change in the collection, use, or disclosure practices to which the parent has previously consented.'*

The 2013 amendments have strengthened accountability by imposing obligations on operators in respect of security practices by service providers and third parties with which it shares information.

> *'§312.8 Confidentiality, security, and integrity of personal information collected from children.*
>
> *The operator must establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children. The operator must also take reasonable steps to release children's personal information only to service providers and third parties who are capable of maintaining the confidentiality, security and integrity of such information, and who provide assurances that they will maintain the information in such a manner.'*

This is a form of strict liability that applies to an app developer 'where it integrates outside services, such as plugins or advertising networks, that collect personal information from its visitors'.[113] An app developer must therefore exercise every possible precaution[114] when integrating software development kits (SDKs) and third party libraries into the app code to verify what personal information of children will be collected and how it will be used and disclosed. At a minimum, app developers must ensure that the terms of service of

[113] Children's Online Privacy Protection Rule; Final Rule Amendments, FR 79(12) Part II (17 January 2013) at 3976–3977. This could include e.g. analytics, MBaaS and cloud storage services for which the app developer pays, and ad libraries and other third-party code integrated into the app (as by doing so the app developer allows another to collect information *directly* from users of the app, and the app developer benefits from that collection through enhanced functionality, increased traffic, and ad revenue).

[114] Ibid. The legal standard imposed is 'strict liability' and there is no 'safe harbour' for exercising reasonable measures or 'due diligence' although the FTC has indicated it will consider the reasonableness of the measures taken in the exercise of its 'prosecutorial discretion'.

third parties include appropriate contractual guarantees for how they will collect and use personal information,[115] although in practice this may not be easy.[116]

Where the operator discloses or 'releases'[117] information to a 'third party',[118] the COPPA Rule requires notice and verified parental consent for the collection, use and disclosure of such information,[119] and requires the operator to make the service available even if parents refuse consent for disclosure to third parties.

> *'§312.5 Parental consent.*
>
> *(a) … (2) An operator must give the parent the option to consent to the collection and use of the child's personal information without consenting to disclosure of his or her personal information to third parties.'*

The potentially unreasonable impact of this provision is limited in that transferring data to service providers or agents to enable them to perform their contractual functions is not a 'disclosure'[120] of information, provided it takes place for 'internal support,'[121]

---

[115] Cf GDPR and Protection of Personal Information Act 4 of 2013 (POPIA) which both refer to using 'contractual means' to ensure that service providers and agents ('operators' in those statutes) process personal information lawfully, but do not directly address sharing with third parties.

[116] As indicated in chapter 2, given the imbalance in bargaining power between app developers and service providers, 'take it or leave it' contract terms are not uncommon, and there is presently very little transparency about actual data practices.

[117] COPPA Rule 16 C.F.R §312. §312.2 '*Release of personal information* means the sharing, selling, renting, or transfer of personal information to any third party'.

[118] Ibid. '*Third party* means any person who is not:
(1) An operator with respect to the collection or maintenance of personal information on the Web site or online service; or
(2) A person who provides support for the internal operations of the Web site or online service and who does not use or disclose information protected under this part for any other purpose.'

[119] As indicated in chapter 2, the imbalance of contractual bargaining power and lack of transparency about data practices applies equally to third parties such as ad networks and ad exchanges making it difficult for app developers to verify that there have been no material changes that require renewed parental consent, and to verify the security and integrity of data stored by third parties as required under 16 CFR §312.5 and §312.8.

[120] COPPA Rule 16 C.F.R §312.2 '*Disclose or disclosure* means, with respect to personal information:
(1) The release of personal information collected by an operator from a child in identifiable form for any purpose, except where an operator provides such information to a person who provides support for the internal operations of the Web site or online service; and
(2) Making personal information collected by an operator from a child publicly available in identifiable form by any means, including but not limited to a public posting through the Internet, or through a personal home page or screen posted on a Web site or online service; a pen pal service; an electronic mail service; a message board; or a chat room'.

[121] Ibid. '*Support for the internal operations of the Web site or online service means:*
(1) Those activities necessary to:
(i) Maintain or analyze the functioning of the Web site or online service;
(ii) Perform network communications;
(iii) Authenticate users of, or personalize the content on, the Web site or online service;
(iv) Serve contextual advertising on the Web site or online service or cap the frequency of advertising;

which would include most app analytics and the collection of user credentials for authenticating users, personalising content or detecting fraud (or other security or integrity risks to the user, site or service).[122] This means that, although the app's privacy policy[123] and a direct notice to parents[124] must indicate what personal information is collected and how it is used, the operator does not need 'verified parental consent'[125] to transfer the information to service providers. Furthermore, if the operator collects only a persistent identifier (and no other personal information) and uses this solely for internal support functions, no notice and consent is required.[126]

Under COPPA an operator is defined as

> *'any person who operates a website located on the Internet or an online service and who collects or maintains personal information from or about the users of or visitors to such website or online service, or on whose behalf such information is collected or maintained ... '* (own emphasis).[127]

(v) Protect the security or integrity of the user, Web site, or online service;
(vi) Ensure legal or regulatory compliance; or
(vii) Fulfill a request of a child as permitted by §312.5(c)(3) and (4);'.
The latter is a reference to collecting contact information *only* for the purpose of replying to specific requests from the child (without notice for one-time requests where the information is immediately deleted, or with notice and verified parental consent in all other cases).

[122] The list is exhaustive of the categories of internal services that qualify for exemption, but a range of activities could be accommodated within each category and no particular technology is prescribed. E.g. apps may use different user authentication techniques. Failure to define terms such as 'personalisation of content' may, however, leave room for profiling activities (as discussed in chapter 2).

[123] COPPA Rule 16 C.F.R §312 §312.4(d) requires that 'a prominent and clearly labelled link to an online notice of its information practices with regard to children' be displayed on the home screen of the app (or the children's area) and each screen where the app collects personal information ('in close proximity to the requests for information'). It must be clear, understandable, written, complete, and without unrelated, confusing, or contradictory material. It must detail what personal information is collected, how it is used and the operator's 'disclosure practices', including whether the app will allow the child to make the information public. It must set out how parents exercise rights to review and delete information and withdraw their consent for future processing, and provide the operator's contact details (name, address, telephone number, and email address).

[124] Ibid. This is a short form notice providing key details (set out in §312.4(c) and a hyperlink to the privacy policy). §312.4(b) provides that the operator 'must make reasonable efforts, taking into account available technology, to ensure that a parent of a child receives direct notice'.

[125] Ibid. §312.5(a) requires that 'verified parental consent' be obtained before collection, use or disclosure and fresh consent is required if there is a 'material change' in such practices. Apps can also comply through voluntary certification by Aristotle International Inc., Children's Advertising Review Unit (CARU), Entertainment Software Rating Board (ESRB), iKeepSafe, kidSAFE, Privacy Vaults Online, Inc. (d/b/a PRIVO) or TRUSTe under the 'COPPA Safe Harbour Program' <https://www.ftc.gov/safe-harbor-program> accessed 4 March 2020.

[126] COPPA Rule 16 C.F.R §312. §312.5(c)(7) 'Where an operator collects a persistent identifier and no other personal information, and such identifier is used for the sole purpose of providing support for the internal operations of the Web site or online service. In such case, there also shall be no obligation to provide notice under §312.4'.

[127] COPPA §6501(2).

The amendment of the COPPA Rule in 2013 introduced a very wide definition of when a person acts 'on behalf of' an operator, to include not just service providers and agents, but any party whose collection of personal information directly from the users of a site or service *benefits the operator*.[128] The FTC has justified this approach on the basis of several federal court cases which have interpreted the phrase 'on behalf of' as including actions done for the benefit of another.[129]

Thus a plug-in or ad network will be accountable as a 'co-operator', in that it will be deemed to be an operator if it obtains the personal information directly from a site directed at children (but only where it has 'actual knowledge' that it is collecting such information).[130] In each case, this would be a question of fact, but the FTC has indicated that in addition to evidence of a direct communication of the 'child-directed nature of its content') by the operator (content provider), if the other service 'recognizes' that the content is child-directed or knows that the information relates to a child through 'an accumulation of other facts', that may suffice.[131]

Thus ad networks and other software providers must carefully consider what personal information (if any) they need to collect and how they will comply with their responsibilities.[132] The FTC has recognised that the ecosystem is complex and there is not a great deal of transparency from advertising 'partners' about their data handling practices, but has taken the view that it was unacceptable for these practices to remain unregulated (what I refer to in this dissertation as an 'accountability gap').[133] This does not extend to platforms such as the App Store and Google Play store, which are not intended to be 'operators' under

---

[128] COPPA Rule 16 C.F.R §312.2 provides 'Personal information is *collected or maintained on behalf of* an operator when:
(1) It is collected or maintained by an agent or service provider of the operator; or
(2) The operator benefits by allowing another person to collect personal information directly from users of such Web site or online service'.

[129] See e.g. *American Postal Workers Union v United States Postal Service* 595 FSupp 1352 (DDC 1984); *Sedwick Claims Management Services v Barrett Business Services Inc* 2007 WL 1053303 (D Or 2007); *United States v Dish Network LLC* 2010 US Dist LEXIS 8957, 10 (CD Ill Feb 3, 2010) and *National Organization for Marriage v Daluz* 654 F3d 115, 121 (1st Cir 2011).

[130] Children's Online Privacy Protection Rule; Final Rule Amendments, FR 79(12) Part II (17 January 2013).

[131] Ibid at 3978.

[132] As third parties may have no direct means of contacting the parents of a child to obtain verified parental consent, they may need to ensure that contracts with app developers oversee the mechanisms by which apps will disclose and obtain consent for the data handling practices.

[133] Children's Online Privacy Protection Rule; Final Rule Amendments, FR 79(12) Part II (17 January 2013).

COPPA for child-directed apps available in the app stores,[134] although there is a strong argument to be made that it should, as they benefit from the mobile apps ecosystem through revenue earned on each app download. It remains to be seen whether Apple and Google would be held liable as operators in respect of their own direct collection of personal information from mobile apps that integrate their APIs (about which there is very little known).

In 2016 the FTC took direct action against Singaporean advertising platform InMobi Pte Ltd[135] for its deceptive representations to app developers,[136] consumers[137] and advertisers that it collected location information only with opt-in consent.[138]

App developers integrated the InMobi SDK to monetise their apps with in-app location-based advertising.[139] They were unable to provide complete information to app users about the collection of location information because the InMobi SDK integration guide for developers contained false representations to the effect that location-based ads were served only if developers included a location permission in the app manifest.[140] On this basis,

---

[134] Ibid. Although such platforms clearly benefit from hosting apps (as discussed in chapter 2) the FTC report makes it clear that they were not intended to become strictly liable for the collection of personal information by those apps. However, platforms are subject to COPPA as operators in their own right to the extent that they collect information about children from their own websites and online services. The FTC has therefore not addressed the question of whether app stores have any legal responsibility to review apps before placing them in the app store. For further discussion of the liability of platforms, see Ingrid Lambrecht, Valerie Verdoodt & Jasper Bellon 'Platforms and Commercial Communications Aimed at Children: A Playground under Legislative Reform?' (2018) 32 (1) *International Review of Law, Computers & Technology* 58–79.

[135] *United States v InMobi Pte Ltd* Case No 3:16-cv-03474 (ND Cal Jun 22, 2016). InMobi was the self-proclaimed world leader in mobile advertising. In February 2015 it reported that its network reached one billion unique mobile devices and served 6 billion ad requests per day.

[136] Ibid (complaint para 28–30). The InMobi SDK integration guide for Android developers stipulated: 'To allow InMobi to show Geo targeted ads, you need to add the ACCESS_COURSE_LOCATION [sic] and ACCESS_FINE_LOCATION permissions'. Likewise, the guide for iOS developers stipulated: 'You can set the user location by using the location methods in the ad request.'

[137] Ibid (complaint para 42). InMobi's privacy policy contained the following misrepresentation: 'WHAT ABOUT CHILDREN? We do not knowingly collect any personal information about children under the age of 13. If we become aware that we have collected personal information about a child under the age of 13, that information will be immediately deleted from our database.'

[138] Ibid (complaint para 43). A special COPPA Policy was disseminated by InMobi misrepresenting that it did not collect information from children for behavioural advertising and had identified all existing publisher sites and apps directed to children to ensure full compliance with the 2013 COPPA Rule amendments.

[139] As explained in chapter 2, collection of location allows for targeted advertising. InMobi offered advertisers the choice of targeting consumers based on their current location (e.g. at a particular shop), defined conditions (e.g. visits airports on Monday mornings) or based on location history for up to the last two months (e.g. lives in an affluent neighbourhood and visited luxury auto dealerships in the last two months). Ads are served in the form of banner ads, interstitial ads and native ads within the app, and can also be retargeted to other sites or apps visited by the user.

[140] As explained in chapter 2, the Android and iOS operating systems (OS) provide application developers with application programming interfaces (APIs) through which they can request access to the on-device GPS (either requesting fine-grained location, providing precise GPS co-ordinates, or a coarse-grained location, giving an

numerous app developers represented to consumers in their privacy policies that consumers have the ability to control the collection and use of location information through app permissions and device location settings.[141] These application developers 'had no reason to know that Defendant tracked the consumer's location and served geo-targeted ads regardless of the consumer's location settings'.[142] Even if app users disabled location services, InMobi inferred their location using information collected about Wi-Fi networks to which the device was connected or was in range.[143] In this way, InMobi was tracking users' location and serving geo-targeted ads, regardless of the application developer's intent to include geo-targeted ads in the application and without the user's knowledge.[144] Following the FTC investigation, InMobi made changes to its SDK and internal systems to ensure that in future it will track location only if the app user has allowed access to the location.[145] With the release of Android 10 and iOS 13, both Google and Apple no longer permit developers to access BSSID and ESSID unless app users have granted location permission.[146]

---

approximate location accurate to within 2000m). The OS only permits access if the user gives consent through a 'permission'. At the time of the complaint in Android v5.1, permissions were granted at install time, and users either had to grant all permissions requested or not install the app. Like iOS, later versions of Android now ask for dangerous permissions (such as location) at runtime, and permissions can be granted individually. Once location permission was granted to the app, the InMobi SDK was automatically privileged with the same permission.

[141] The user could either deny the location permission (which at that time in Android meant not installing the app) or the user could turn off location services in the device settings. The complaint is not addressed to app developers. They must ensure of course that they disclose to users that location is collected but also all the ways that it is used and who it is disclosed to, including its use for serving targeted advertising.

[142] *United States v InMobi Pte Ltd* (complaint, para 37).

[143] As explained in chapter 2, app developers may need to request Wi-Fi ESSID (network name), BSSID (a unique identifier), and signal strength to make sure the app is connected to the network before performing a function. InMobi did not inform developers that it would also collect the Wi-Fi information to serve targeted ads.

[144] A user who restricted location settings on the device would probably not know that Wi-Fi can disclose location. Note that although the FTC complaint states that in Android the 'Access Wi-Fi state' or 'Change Wi-Fi state' permission (necessary to access this information) would be requested on installation, this has changed. Android has reclassified these as 'normal' permissions. As explained in chapter 2, a normal permission is granted automatically without notice to the user. Android Developers, 'Permissions Overview' <https://developer.android.com/guide/topics/permissions/overview#dangerous_permissions> accessed 31 August 2019.

[145] *United States v InMobi Pte Ltd* (complaint para 27).

[146] However in Android 10 and iOS 13 both platforms restricted user tracking by explicitly requiring that apps have permission to access location in order to obtain information on cellular network, Wi-Fi and Bluetooth connections. Android Developers, 'Privacy changes in Android 10' (27 December 2019) <https://developer.android.com/about/versions/10/privacy/changes> accessed 19 February 2020. Apple Developer Centre, 'CNCopyCurrentNetworkInfo' (2020) <https://developer.apple.com/documentation/systemconfiguration/1614126-cncopycurrentnetworkinfo> accessed 8 March 2020.

V SMALL BUSINESSES

A 'small' business is ordinarily defined by reference to size of the entity (measured by number of employees or annual turnover). In the US, an app developer would be a 'small entity' if it has fewer than 1 000 employees.[147] Most app developers are small entities.[148] In the US, the Regulatory Flexibility Act (1980) (RFA)[149] requires federal agencies to publish an analysis of whether any final Rule will have 'a significant economic impact on a substantial number of small entities'.[150] The FTC was cognisant of the 'potential burden' created by the COPPA amendments, particularly for small app developers,[151] which will require them to engage professional legal and technical skills to implement COPPA protections,[152] and will review these burdens again in its latest review.[153]

COPPA applies to all 'operators' regardless of the size of the entity. This is consistent with the FTC's view that it is not appropriate to exempt small entities from legislative compliance as their activities could constitute just as great a risk to user privacy as the activities of a larger entity.[154]

---

[147] US Small Business Administration, 'Table of Size Standards' (19 August 2019) <https://www.sba.gov/document/support--table-size-standards> accessed 5 March 2020. App developers would be classified under North American Industry Classification System (NAICS) code 519130 'Internet Publishing and Broadcasting and Web Search Portals'.

[148] Children's Online Privacy Protection Rule; Final Rule Amendments, FR 79(12) Part II (17 January 2013) at 4000 estimated that 90% of businesses affected by the COPPA rule would be small entities. Their report refers to a figure of 500 employees (which applied before the US size standard was amended).

[149] Regulatory Flexibilty Act of 1980, 5 U.S.C. §601–612 (2018).

[150] RFA §605(b).

[151] Children's Online Privacy Protection Rule; Final Rule Amendments, FR 79(12) Part II (17 January 2013) at 3977, also noting that public comments submitted to the FTC expressed this concern but did not identify the additional costs or attempt to quantify them.

[152] Ibid at 4000.

[153] Request for Public Comment on the Federal Trade Commission's Implementation of the Children's Online Privacy Protection Rule, FR 84(143) (25 July 2019) at 35843–35844.

[154] Children's Online Privacy Protection Rule; Final Rule Amendments, FR 79(12) Part II (17 January 2013) at 4001. See e.g. *United States v RockYou Inc* Case No 3:12–cv–01487–SI (ND Cal Mar, 27, 2012) (32 million account names and passwords compromised); *United States v Godwin* Case No 1:11–cv–03846–JOF (ND Ga Feb 1, 2012) (5600 public social networking profiles created by children); *United States v. W3 Innovations LLC* supra (32 000 downloads), *United States v Industrious Kid Inc* Case No CV–08–0639 (ND Cal,filed Jan 28, 2008) (10500 social networking profiles created by children – full name, email address, gender, age, and photographs and blog entries were collected, and 'Imbee' business cards with a name, photo and URL to the blog were posted to children without parental consent); *United States v Xanga.com Inc* Case No 06–CIV–6853 (SDNY Sept 11, 2006) (1.7 million public blogging accounts opened by children); *United States v Bonzi Software Inc* Case No CV–04–1048 (CD Cal Feb 17, 2004)(a 'virtual assistant' for desktops offered as freeware, but collected personal information including birthdates from 1000s of children, and served targeted advertising); *United States v Looksmart Ltd* Case No 01–605–A (ED Va Apr 18, 2001)); and *United States v Bigmailbox.Com Inc* Case No 01–606–B (ED Va Apr 18, 2001).

In its Privacy Framework, the FTC proposed a novel approach that exempts entities who do not collect any sensitive data, have fewer than 5 000 consumers per year, and do not share any data with third parties.[155] To assist small entities further with COPPA compliance, the FTC website contains a six-step compliance plan,[156] with an explainer video[157] and additional resources.[158]

VI CALIFORNIA ONLINE PRIVACY PROTECTION ACT (2004) (CalOPPA)

(a) Origin and background

California was the first state to enact a general consumer privacy law, with CalOPPA coming into effect on 1 July 2004.[159] In 2012, the California Attorney-General stated that CalOPPA

> *'requires mobile applications that collect personal data from California consumers to conspicuously post a privacy policy or other statement describing the app's privacy practices that provides clear and complete information regarding how personal data is collected, used and shared'*.[160]

The California AG is empowered to seek injunctive relief and a fine of $2500 per violation (being each visit to the online service by a user)[161] if an operator does not post a privacy policy within 30 days of being notified that it is in violation of CalOPPA.[162]

---

[155] Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for businesses and policymakers* at 14–15. Such 'first party' collection of non-sensitive data would, it is submitted, include personal information such as persistent identifiers used for internal support functions even if these functions are outsourced to a service provider, e.g. use of an app analytics provider. However, where that provider will make further use of the data, then the exemption will not apply, as this is a third party disclosure of data.

[156] Federal Trade Commission, *Children's Online Privacy Protection Rule: A Six-Step Compliance Plan for Your Business* (June 2017).

[157] Federal Trade Commission, 'Protecting Children's Privacy Under COPPA ' (*Video*, 1 July 2013) <https://www.ftc.gov/news-events/audio-video/video/protecting-childrens-privacy-under-coppa> accessed 15 May 2020.

[158] The website has a Frequently Asked Questions section, and links to COPPA, the COPPA Rule, and workshops, statements and staff reports related to children's privacy. This includes a report on ed tech: Federal Trade Commission, 'Student Privacy and Ed Tech' (1 December 2017) <https://www.ftc.gov/news-events/events-calendar/2017/12/student-privacy-ed-tech> accessed 5 March 2020.

[159] CalOPPA s 22579.

[160] State of California Office of the Attorney General, *Agreement to Strengthen Privacy Protections for Users of Mobile Applications* (22 February 2012).

[161] Enforcement, Cal. Bus. & Prof. Code §§17200–17210 at §17206. The fine could thus be substantial depending on the number of times the mobile app has been downloaded.

[162] CalOPPA §22575(a).

(b) Personal Information

The definition of 'personally identifiable information' (PII) mirrors the definition of 'personal information' in COPPA, save that it applies to an individual *consumer*[163] residing in California, and is subject to the provisos that the information is 'collected online *by the operator from that individual* and maintained by the operator in an accessible form'.[164] Although there is no case law, the California AG has taken the view that this includes persistent device identifiers,[165] and this was included in the complaint against the Fly Delta app.[166]

(c) Operator

Although CalOPPA also uses the term 'operator',[167] it is restricted to the *owner*[168] of a commercial website or online service that both collects *and* maintains personally identifiable information about consumers resident in California.[169] If a South African mobile application

---

[163] Ibid §22577(d). The term 'consumer' is defined as 'any individual who seeks or acquires, by purchase or lease, any goods, services, money, or credit for personal, family, or household purposes'.

[164] Ibid §22577(a). The term 'personally identifiable information' is defined as 'individually identifiable information about an individual consumer collected online by the operator from that individual and maintained by the operator in an accessible form, including any of the following:
(1) A first and last name.
(2) A home or other physical address, including street name and name of a city or town.
(3) An e-mail address.
(4) A telephone number.
(5) A social security number.
(6) Any other identifier that permits the physical or online contacting of a specific individual.
(7) Information concerning a user that the Web site or online service collects online from the user and maintains in personally identifiable form in combination with an identifier described in this subdivision'.

[165] State of California Office of the Attorney General, *Privacy on the Go: Recommendations for the Mobile Ecosystem* (2013) at 2 and 6.

[166] *Harris v Delta Airlines Inc* 247 CalApp4th 884 (2016) at note 5 records that in its appeal brief, the State of California alleged that Delta had not disclosed in any privacy policy its collection of PII in the form of 'universal device identification, which "uniquely and statically identifies the mobile device and user"'. The original complaint also asserted that the Fly Delta app collected the following PII: '(a) geo-location data (GPS); (b) photographs; (c) user's full name; (d) street addresses (residential and billing); (e) telephone numbers (including cell, fax, and pager); (f) email addresses; (g) Delta Sky Miles account number and flight information; (h) credit/debit card numbers and expiration dates; (i) date of birth; (j) gender; (k) traveller number; (l) travel-related information, such as travel company, emergency contacts, seating preferences, medical needs and dietary requests; (m) passport number, nationality, country of residence; (n) corporate contract, employer or affiliation.'

[167] CalOPPA §22577(c). The term 'operator' is defined as 'any person or entity that owns a Web site located on the Internet or an online service that collects and maintains personally identifiable information from a consumer residing in California who uses or visits the Web site or online service if the Web site or online service is operated for commercial purposes. It does not include any third party that operates, hosts, or manages, but does not own, a Web site or online service on the owner's behalf or by processing information on behalf of the owner.'

[168] COPPA, on the other hand, defines an operator as the person who 'operates' the website or online service.

[169] While COPPA refers to collecting *or* maintaining personal information.

owner[170] collects information from California residents, it would be required to comply with CalOPPA.

(d) Data Protection Principles

CalOPPA deals only with the requirement of notice, and requires that a privacy policy be 'conspicuously' posted. In the case of a mobile app, which is an online service governed by CalOPPA. This means that it must be made 'available' by 'reasonably accessible means'.[171] This would require posting a link[172] to the privacy policy in the app store and in the app itself where the user would see it when first opening the app,[173] and where it would be accessible later in the app settings or on an account dashboard, and on the app's associated website.[174] If a privacy policy is displayed on a website but does not clearly refer to the PII collected by an associated mobile app, this does not suffice.[175]

The protections under CalOPPA are weaker than COPPA in five key respects:

1. The privacy policy must identify the categories of personally identifiable information collected and the categories of third parties with whom it may be shared.[176] Save as set out below, there is no requirement to specify how the

[170] As explained in chapter 2, the mobile application owner will often (but not always) be the mobile application developer.
[171] CalOPPA §22577(b)(5) provides: 'The term "conspicuously post" with respect to a privacy policy shall include posting the privacy policy through any of the following: … (5) In the case of an online service, any other reasonably accessible means of making the privacy policy available for consumers of the online service'.
[172] Ibid. The link must be 'so displayed that a reasonable person would notice it' (§22577(b)(4)). This could include using an icon containing the word privacy and distinguished from the background e.g. by a contrasting colour (§22577(b)(2)), or a text link containing the word privacy in capital letters and distinguished from the background e.g. must have same or larger font size, and can use contrasting type, font, colour or a symbol (§22577(b)(3)).
[173] State of California Office of the Attorney General, *Privacy on the Go: Recommendations for the Mobile Ecosystem* at 10 recommends that it is available in the app store so that it can be reviewed before the app is installed and that there is a link in the app ('e.g. on controls/settings page). This recommendation must be read with the legislative requirement that the posting be 'conspicuous'. It is submitted that to have a privacy policy link available only in an obscure app setting but not make it easy to find would not be 'conspicuous'.
[174] CalOPPA §22577(b)(1) requires that the actual policy or a hyperlink (as described above) must be posted 'on the homepage or the first significant page' of a commercial website. Cf COPPA Rule 16 C.F.R §312 which additionally requires that a link to the privacy policy be displayed 'at each place on the website or online service where personal information is collected'.
[175] *Harris v Delta Airlines Inc*. The State's complaint alleged that Delta's privacy policy available on its website did not outline what PII was collected by the Fly Delta app (including geo-location and photographs). The case was dismissed on the grounds that the federal Airline Deregulation Act of 1978, 49 U.S.C. § 1371 (2018) pre-empted CalOPPA. There is accordingly no final decision on where a mobile app privacy policy must be displayed.
[176] CalOPPA §22575(b)(1). Cf COPPA Rule 16 C.F.R §312.4(b) which requires that '[a]n operator must make reasonable efforts, taking into account available technology, to ensure that a parent of a child receives direct notice of the operator's practices with regard to the collection, use, or disclosure of personal information from children,

information will be used by the operator and such third parties, and there is no express requirement that it be clear and understandable, and have no unrelated, confusing or contradictory content.[177]

2. Although best practice for mobile application developers would be to use a 'clickwrap'[178] agreement, by including the privacy policy link alongside an icon or check-box which the user must click to indicate consent, on the app's registration page before first use,[179] this is not mandatory under CalOPPA.[180] There is no requirement to confirm that the notice has come to the attention of consumers and to verify that they have consented to the practices disclosed before collecting the information.[181] Similarly, the policy must describe how changes will be communicated and stipulate their effective date, but the onus remains on the consumer to check for updates.[182]

3. There is no right to review and request changes to information, but if the operator voluntarily provides such a mechanism, it must describe the process.[183]

---

including notice of any material change in the collection, use, or disclosure practices to which the parent has previously consented'.

[177] cf COPPA Rule 16 C.F.R §312.4(a).

[178] A 'clickwrap' agreement derives its name from the fact that the user takes affirmative action to indicate their assent to the operator's standard terms and conditions by clicking on an icon or check-box. The term originated in the so-called 'shrinkwrap' agreement, where notice of software licence agreements and terms of use was displayed on the packaging of the software and by opening the shink-wrapper and installing the software, the user implied agreed to those terms. See Tana Pistorius, 'Click-wrap and Web-wrap Agreements' (2004) 16 *S Afr Mercantile LJ* 568–576.

[179] TermsFeed, 'CalOppa: Your Guide to Creating a Compliant Privacy Policy' <https://www.termsfeed.com/blog/caloppa-compliant-privacy-policy/> accessed 9 March 2020.

[180] The provisions of CalOPPA mandate a 'browse-wrap' (or web-wrap) agreement, where by virtue of prominent notice of the terms use of the website or online service constitutes implied consent to the terms without any affirmative action by the user.

[181] Cf COPPA Rule 16 C.F.R §312.5.

[182] CalOPPA §22575(b)(3) & (4). State of California Office of the Attorney General, *Privacy on the Go: Recommendations for the Mobile Ecosystem* at 10, recommends that the privacy policy be hosted in the developer's browser to facilitate updates. This is much less stringent than COPPA Rule 16 C.F.R §312.4(b), which requires a fresh direct notice to parents whenever there is a 'material change' in data practices for which consent was previously obtained.

[183] CalOPPA §22575(b)(2). Cf COPPA Rule 16 C.F.R §312.6.

4. With effect from 1 January 2014,[184] the privacy policy must disclose its tracking[185] and sharing of consumer information.[186] However, an operator is not prohibited from incentivising app users to share more information than is required for the app to function,[187] nor is it prohibited from making use of the app conditional upon consent to third party disclosure.[188]

5. If an app developer makes representations in its privacy policy about how it safeguards personal information, it can be held accountable for knowingly or negligently failing to implement such safeguards.[189] However, CalOPPA does not stipulate that the operator is responsible for the security, integrity and confidentiality of a customer's personal information and does not specify what notice (if any) must be given to consumers about its security practices. [190]

VII CALIFORNIA CONSUMER PRIVACY PROTECTION ACT (2018) (CCPA)

(a) Origin and background

The CCPA came into effect on 1 January 2020. It does not repeal CalOPPA, but provides additional data protection for consumers in relation to covered businesses.

---

[184] Bill to amend §22575 of Cal. Bus. & Prof. Code, A.B. 370, 2013–2014, ch.390, 2013, Cal. Stat. (effective 1 January 2014).

[185] CalOPPA §22575(b)(5) requires the operator to '[d]isclose how the operator responds to Web browser "do not track" signals *or other mechanisms that provide consumers the ability to exercise choice regarding the collection of personally identifiable information about an individual consumer's online activities over time and across third-party Web sites or online services*, if the operator engages in that collection'. As discussed in chapter 2, in the mobile applications context these are limited to permissions given to the app governed by the OS.

[186] Ibid §22575(b)(6) 'whether other parties may collect personally identifiable information about an individual consumer's online activities over time and across different Web sites when a consumer uses the operator's Web site or service'.

[187] cf COPPA Rule 16 C.F.R §312.7.

[188] cf COPPA Rule 16 CFR §312.5(a)(2).

[189] CalOPPA §22576 provides: 'An operator of a commercial Web site or online service that collects personally identifiable information through the Web site or online service from individual consumers who use or visit the commercial Web site or online service and who reside in California shall be in violation of this section if the operator fails to comply with the provisions of Section 22575 or with the provisions of its posted privacy policy in either of the following ways:
(a) Knowingly and willfully.
(b) Negligently and materially'.

[190] Cf COPPA Rule 16 C.F.R §312.8.

(b) Personal Information

A covered business must disclose to a 'consumer'[191] all 'personal information',[192] namely:

> *'[I]nformation that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household. Personal information includes, but is not limited to, the [a non-exhaustive list of 10 information categories and inference drawn from that information] if it identifies, relates to, describes, is reasonably capable of being associated with, or could be reasonably linked, directly or indirectly, with a particular consumer or household:'.*

In providing that 'personal information' is information that can be linked either to a particular consumer or to *a household*,[193] whether directly or indirectly,[194] the definition is wider than other statutory definitions.[195]

The ten information types referred to in the definition do not form an exhaustive list, and are comparable to the types of personal information covered by other statutes. To comply with CCPA, a mobile application developer's privacy policy must describe which of each of these categories of personal information is collected:[196]

> *'(A) Identifiers such as a real name, alias, postal address, unique personal identifier, online identifier, internet protocol address, email address, account name, social security number, driver's license number, passport number, or other similar identifiers.*
>
> *(B) Any categories of personal information described in subdivision (e) of Section 1798.80.*

---

[191] CCPA §1798.140(g). The term 'consumer' is defined as 'a natural person who is a California resident, as defined in Section 17014 of Title 18 of the California Code of Regulations, as that section read on September 1, 2017, *however identified, including by any unique identifier*' (own emphasis). Also see §1798.140 (o)(1)(A) & (G) which includes any 'unique personal identifier', 'online identifier' and 'geolocation data' as personal information.

[192] Ibid §1798.140(o)(1).

[193] The term 'household' is not defined.

[194] This is comparable to GDPR art4(1) which provides that 'an identifiable natural person is one who can be identified, directly or indirectly'.

[195] Compare the definition of personal information in COPPA Rule 16 C.F.R §312.2 'individually identifiable information about an individual collected online'; CalOPPA §22577(a) 'individually identifiable information about an individual consumer collected online by the operator from that individual and maintained by the operator in an accessible form'; GDPR ar t4(1) 'any information relating to an identified or identifiable natural person'; and POPIA s 1 ' information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person'.

[196] CCPA §1798.100(b) (discussed further below).

(C) Characteristics of protected classifications under California or federal law.

(D) Commercial information, including records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies.

(E) Biometric information.

(F) Internet or other electronic network activity information, including, but not limited to, browsing history, search history, and information regarding a consumer's interaction with an internet website, application, or advertisement.

(G) Geolocation data.

(H) Audio, electronic, visual, thermal, olfactory, or similar information.

(I) Professional or employment-related information.

(J) Education information, defined as information that is not publicly available personally identifiable information as defined in the Family Educational Rights and Privacy Act (20 U.S.C. Sec. 1232g; 34 C.F.R. Part 99).

(K) Inferences drawn from any of the information identified in this subdivision to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.'[197]

The app must therefore have a comprehensive privacy policy available on the app store and the app's associated website before download, as well as within the app in settings or an account dashboard.[198] An app can also make use of the kinds of short 'just in time' notifications (with links to the privacy policy, where possible) recommended in regulatory guidelines, to highlight collection, use or disclosure of 'sensitive' information,[199] or practices that would be 'unexpected'.[200]

---

[197] Ibid §1798.140(o).

[198] Ibid §1798.135(a)(1) requires a 'clear and conspicuous' notice via a link on the 'homepage', which for the purpose of a mobile app is defined (in §1798.140(l) as 'the application's platform page or download page, a link within the application, such as from the application configuration, "About," "Information," or settings page, and any other location'.

[199] Ibid. Does not define a category of 'sensitive' information, but as discussed earlier, it is associated with app store classifications that require users to grant run time permissions for 'dangerous permissions' (e.g. location) and with information about children, health, sexual, religious or political preferences and financial information.

[200] State of California Office of the Attorney General, *Privacy on the Go: Recommendations for the Mobile Ecosystem* at 13. COPPA, CalOPPA and CCPA all carve out exceptions for uses that are reasonably consistent

The term 'unique identifier' is particularly important in the context of mobile apps, which routinely collect a variety of persistent and semi-persistent identifiers, both for internal operations and to generate advertising revenue. All of these, including resettable advertising identifiers, are expressly included in the scope of the CCPA, and the collection, use and disclosure of such identifiers must be explained. The term 'unique identifier' is comprehensively defined:[201]

> *'"Unique identifier" or "Unique personal identifier" means a persistent identifier that can be used to recognize a consumer, a family, or a device that is linked to a consumer or family, over time and across different services, including, but not limited to, a device identifier; an Internet Protocol address; cookies, beacons, pixel tags, mobile ad identifiers, or similar technology; customer number, unique pseudonym, or user alias; telephone numbers, or other forms of persistent or probabilistic identifiers that can be used to identify a particular consumer or device. For purposes of this subdivision, "family" means a custodial parent or guardian and any minor children over which the parent or guardian has custody.'*[202]

The privacy policy should thus disclose whether the app collects, uses or discloses 'pseudonymised'[203] PII, including a 'screen name' or 'user name'[204] that is an alias (or pseudonym) and not the consumer's real name. In respect of all PII, the privacy policy should make it clear whether the uses of data fall within what the customer would reasonably expect in the context of the app's apparent functions, or outside those parameters (including whether the developer or a third party may retain the information in a record, as part of a profile, of for other purpose, for longer than the business purpose of the app requires).

---

with the context in which the information is collected, and notice must be carefully worded to ensure customers are informed about other collection, use and disclosure practices that they may not reasonably expect.

[201] Cf POPIA s 1 which includes in the definition of 'personal information' the term 'online identifier' or 'other particular assigned to an individual' but contains no further definition making it clear that the term includes a device identifier. It remains open to argue cogently that under POPIA a device identifier is personal information as it can be linked to an identifiable individual.

[202] CCPA §1798.140(x) read with (p) which defines a 'probabilistic identifier' as 'the identification of a consumer or a device to a degree of certainty of more probable than not based on any categories of personal information included in, or similar to, the categories enumerated in the definition of personal information.'

[203] Ibid §1798.140(r). '"Pseudonymize" or "Pseudonymization" means the processing of personal information in a manner that renders the personal information no longer attributable to a specific consumer without the use of additional information, provided that the additional information is kept separately and is subject to technical and organizational measures to ensure that the personal information is not attributed to an identified or identifiable consumer.'

[204] See discussion of 'screen name', 'user name' and 'online identifier' under COPPA Rule 16 C.F.R §312 above.

A privacy policy must also specify what 'biometric information',[205] 'health insurance information',[206] 'education information'[207] and 'financial information'[208] is collected. Mobile app developers must also carefully consider, before drafting a privacy policy, whether they will infer[209] any of the above information, or any other personal information (including sensitive information about location or sexual, religious or political preferences) from the information collected.

De-identified, aggregated and publicly available information is not PII and is thus not covered by the CCPA.[210] However, a privacy policy should provide an explanation about whether it 'deidentifies'[211] or 'aggregates'[212] PII, such as for app analytics. Where that

---

[205] CCPA §1798.140(b). 'Biometric information' is defined as 'an individual's physiological, biological, or behavioral characteristics, including an individual's deoxyribonucleic acid (DNA), that can be used, singly or in combination with each other or with other identifying data, to establish individual identity. Biometric information includes, but is not limited to, imagery of the iris, retina, fingerprint, face, hand, palm, vein patterns, and voice recordings, from which an identifier template, such as a faceprint, a minutiae template, or a voiceprint, can be extracted, and keystroke patterns or rhythms, gait patterns or rhythms, and sleep, health, or exercise data that contain identifying information'. This will include fitness and sleep tracker apps, and apps using biometric access control.

[206] Ibid §1798.140(k). 'Health insurance information' is defined as 'a consumer's insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the consumer, or any information in the consumer's application and claims history, including any appeals records, if the information is linked or reasonably linkable to a consumer or household, including via a device, by a business or service provider.' It would also be necessary for health apps to comply with HIPAA.

[207] A full discussion of FERPA is beyond the scope of this dissertation but it broadly covers an 'educational record' directly related to a 'student' kept by (or on behalf of) any US Department of Education funded educational institution. Many 'ed tech' mobile apps would thus need to comply not only with CCPA but also with FERPA.

[208] Apps collecting credit card details would need to comply with the Payment Card Industy (PCI) Security Standards Council, *PCI Data Security Standard v3.2* (2016) and a mobile app developed for a 'financial institution' would need to comply with the GLBA.

[209] CCPA §1798.140(m). '"Infer" or "inference" means the derivation of information, data, assumptions, or conclusions from facts, evidence, or another source of information or data.'

[210] Ibid §1798.140(o)(3) '"Personal information" does not include consumer information that is deidentified or aggregate consumer information.'

[211] Ibid §1798.140(h). Information has been 'deidentified' and is no longer 'personal information' when it 'cannot reasonably identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a particular consumer'. This is subject to the proviso that the business does not attempt to reidentify the data and implements technical safeguards and business protocols to prohibit reidentification of the consumer, including preventing 'inadvertent release of deidentified information'. As such, the definition is comparable in all material respects to the concept of anonymised data under GDPR and the concept of 'deidentified' information under POPIA.

[212] CCPA §1798.140(a). The term 'aggregate consumer information' must be distinguished from de-identified data. Aggregate data is defined as 'information that relates to a group or category of consumers, from which individual consumer identities have been removed, that is not linked or reasonably linkable to any consumer or household, including via a device.' Thus not only has the information had all identifiers removed in such a way that it cannot be linked to an individual, but the information has been combined to present information only about the group or category in such a way that no particular individual can be identified.

'processing'[213] happens off the device, this will require some explanation of how long the information is retained in a personally identifiable form and what encryption (and other security safeguards) are applied to the PII in transfer to, and storage on, the servers of the app developer or its service provider. The privacy policy must also indicate whether 'publicly available information'[214] is linked to any other PII collected, and how that information is used or disclosed.[215]

(c) Business

A 'business' covered by the CCPA covers a for-profit entity[216] doing business in California[217] that 'collects'[218] the PII of a 'consumer' resident in California, or on whose behalf that information is collected, and 'that *alone, or jointly with others, determines the purposes and means of the processing* of consumers' personal information collected'.[219]

A mobile application developer (and app owner) determines the purpose and means of processing through the app code, even where it does so jointly with others by integrating third party APIs, SDKs and ad libraries.

However, the CCPA will apply only to mobile application developers that meet at least one of the following thresholds to be included in the definition of 'business':

1. has annual gross revenues in excess of twenty-five million dollars ($25 000 000);[220]

---

[213] Ibid §1798.140(q). 'Processing' is defined as 'any operation or set of operations that are performed on personal data or on sets of personal data, whether or not by automated means'. This would include the use of anonymization techniques and aggregation algorithms.
[214] Ibid §1798.140(o)(2). 'Publicly available information' includes only information 'lawfully made available from federal, state, or local government records' and expressly excludes biometric information collected without a consumer's knowledge. Thus collection and use of PII by facial recognition software or other biometric systems, must be disclosed and requires consumer consent.
[215] Deidentified and aggregated consumer information (by definition) may not be linked to a consumer.
[216] CCPA §1798.140(c)(1). The definition includes '[a] sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners.' §1798.140(c)(2) extends the definition further to include an entity that controls or is controlled (as defined) by such a business.
[217] This would include a foreign mobile app developer whose app is downloaded by California residents.
[218] CCPA §1798.140(e) '"Collects," "collected," or "collection" means buying, renting, gathering, obtaining, receiving, or accessing any personal information pertaining to a consumer by any means. This includes receiving information from the consumer, either actively or passively, or by observing the consumer's behavior'. This would cover personal information collected via user input and personal information automatically collected by the app.
[219] Ibid §1798.140(c)(1). The wording mirrors the definition of a 'data collector' under GDPR and 'responsible party' under POPIA (POPIA).
[220] CCPA §1798.140(c)(1)(A), which will be adjusted by the consumer price index every odd-numbered year in terms of §1798.185(a)(5).

2. has 50 000 downloads (of its total suite of online services) annually;[221]
3. is monetised primarily by selling PII (which does not include auditing of ad impressions for purposes of calculating ad revenue).[222]

A mobile app developer which has a suite of related apps, or other online services, would have to consider both the total number of consumers or households *and* the total number of devices reached, including smartphones, tablets or wearables.[223] This means that where one consumer or household installs an app across multiple devices, the mobile app developer could quickly reach the CCPA threshold without 50 000 individual consumers or households.

Although the monetary threshold and size threshold would not apply to small app developers, the term 'business' may still extend to many mobile application developers of free apps that rely on behaviourally targeted advertising[224] for 50% or more of their revenue. The definition of 'sell' is broad and includes any transfer of PII, which, as indicated above, includes a unique device identifier, for valuable consideration.[225] As explained in chapter 2, when a mobile app integrates an ad library, it is paid by the ad network for advertising displayed in the app, and thus the transfer of a unique device identifier to facilitate targeted behavioural advertising could be said to be for valuable consideration. It will thus be classified as 'selling' PII, and if the mobile app developer earns 50% of more of its revenue from such advertising, it must comply with the further requirements for customer notice, review and deletion of PII contained in the CCPA.

---

[221] Ibid §1798.140(c)(1)(B) refers to a business that '[a]lone or in combination, *annually* buys, *receives* for the business's commercial purposes, sells, or shares for commercial purposes, *alone or in combination, the personal information of 50,000 or more consumers, households, or devices*' (own emphasis).
[222] Ibid §1798.140(c)(1)(C) refers to a business that '[d]erives 50 percent or more of its annual revenues from selling consumers' personal information.'
[223] §1798.140(j) defines 'device' as '"[d]evice" means any physical object that is capable of connecting to the internet, directly or indirectly, or to another device'.
[224] These terms were explained in chapter 2 to refer to ads that served based on interests determined by the type of app being used (contextual) or additional PII (such as geo-location) used to infer interest from user behaviour. These earn significantly more revenue than 'generic' ads but may also appeal to customers as they see only ads that they are likely to find relevant.
[225] CCPA §1798.140(t)(1) provides that '"Sell," "selling," "sale," or "sold," means selling, renting, *releasing, disclosing, disseminating, making available, transferring, or otherwise communicating* orally, in writing, or by electronic or other means, a consumer's personal information by the business to another business or a third party for *monetary or other valuable consideration*'.

Furthermore, an app developer that does *not* rely on behaviourally targeted advertising but still collects unique device identifiers (or other PII) for the purposes of calculating revenue from generic or contextual in-app advertising, must:

1. notify app users of this collection and use of PII, and
2. have a written contract with the advertising network that restricts the collection of PII to the minimum necessary for counting ad impressions, and contractually prohibits the ad network from retaining, using or disclosing the PII for any other purpose.

This analysis follows from the CCPA's provision that a transfer of PII to a 'service provider'[226] does not constitute selling, provided that notice is given to customers about the transfer and the service provider does not 'further use, collect or sell' the customer's PII, save to the extent that is 'necessary to perform the business purpose'.[227] The term 'business purpose'[228] is carefully delineated to specified internal purposes necessary for the operation of

[226] Ibid §1798.140(v). The term 'service provider' is defined as 'a sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners, *that processes information on behalf of a business* and to which the business discloses a consumer's personal information for a business purpose pursuant to a written contract, provided that the contract prohibits the entity receiving the information from retaining, using, or disclosing the personal information for any purpose other than for the specific purpose of performing the services specified in the contract for the business, or as otherwise permitted by this title, including retaining, using, or disclosing the personal information for a commercial purpose other than providing the services specified in the contract with the business'.

[227] Ibid §1798.140(t)(2): 'For purposes of this title, a business does *not* sell personal information when: … (C) The business uses or shares with *a service provider* personal information of a consumer that is *necessary to perform a business* purpose if both of the following conditions are met:
(i) The business has provided *notice* of that information being used or shared in its terms and conditions consistent with Section 1798.135.
(ii) *The service provider does not further collect, sell, or use the personal information of the consumer* except as necessary to perform the business purpose;' (own emphasis).

[228] Ibid §1798.140(d). The term 'business purpose' is defined as 'the use of personal information for the business's or a service provider's operational purposes, or other notified purposes, provided that the use of personal information shall be reasonably necessary and proportionate to achieve the operational purpose for which the personal information was collected or processed or for another operational purpose that is compatible with the context in which the personal information was collected. The definition continues to list several purposes. Although it does not contain any express indication that the list is a closed list, there is no catch-all provision, nor is there any other textual indication that additional functions interpreted ejusdem generis would be regarded as 'business purposes'. The purpose appears to be to restrict business purposes to those clearly specified functions set out in the statute.

the service such as security,[229] debugging,[230] provision of the service,[231] product development[232] and system maintenance.[233] It also includes provision for '[a]uditing related to a current interaction with the consumer and concurrent transactions, including, but not limited to, *counting ad impressions to unique visitors, verifying positioning and quality of ad impressions, and auditing compliance with this specification and other standards*'.[234] Further, the term 'business purpose' includes 'short term' and 'transient' use of PII for 'contextual customization' of ads shown within the mobile app.[235] However, simply because in-app ads may be configured to require the user to take some action (such as opening or closing an interstitial ad displayed in a pop-up window), this does not amount to the user instructing the app developer to share its PII with advertisers.[236]

The definition of 'business purpose' excludes any profiling of consumers which may be used to serve ads to them outside the app (i.e. when they visit other websites or use other apps).[237] In such cases, PII (including a unique device identifier and possibly other PII such as geo-location information) is transmitted to the ad network, which may transfer it to advertisers in the network. Both the ad network and individual advertisers are a 'third party'.[238] Even the transfer of information to service providers for a business purpose will be regarded as a 'sale' of personal information to a third party if stringent contractual safeguards and an

---

[229] Ibid §1798.140(d)(2) refers to 'Detecting security incidents, protecting against malicious, deceptive, fraudulent, or illegal activity, and prosecuting those responsible for that activity'.
[230] Ibid §1798.140(d)(3) refers to 'Debugging to identify and repair errors that impair existing intended functionality'.
[231] Ibid §1798.140(d)(5) refers to 'Performing services on behalf of the business or service provider, including maintaining or servicing accounts, providing customer service, processing or fulfilling orders and transactions, verifying customer information, processing payments, providing financing, providing advertising or marketing services, providing analytic services, or providing similar services on behalf of the business or service provider.'
[232] Ibid §1798.140(d)(6) refers to 'Undertaking internal research for technological development and demonstration'.
[233] Ibid §1798.140(d)(7) refers to 'Undertaking activities to verify or maintain the quality or safety of a service or device that is owned, manufactured, manufactured for, or controlled by the business, and to improve, upgrade, or enhance the service or device that is owned, manufactured, manufactured for, or controlled by the business'.
[234] Ibid §1798.140(d)(1). In other words CCPA expressly provides for 'advertising attribution' as a business purpose'.
[235] Ibid. §1798.140(d)(4) quoted above. Pursuant to §1798.140(t)(2)(B), if an app developer uses a device identifier to inform an ad network that a customer has opted out of receiving behaviourally targeted advertising, this would not amount to the sale of PII.
[236] Ibid §1798.140(t)(2)(A) provides that PII is not sold if the customer uses or directs the business to intentionally disclose PII to a third party. However, the customer must intend this transfer to happen. Further, the sub-section provides that 'Hovering over, muting, pausing, or closing a given piece of content does not constitute a consumer's intent to interact with a third party'.
[237] Ibid.
[238] Ibid §1798.140(w).

explicit certification from the service provider are not in place.[239] It is clear that advertisers do not meet these criteria, as the raison d'être of advertisers is the commercial use of personal information to generate advertising revenue, and this is not a service in the contract between the business (app developer) and consumer (app user).[240]

Thus, a mobile app relying for 50% or more of its revenue from serving in-app generic or contextual adverts, and using a unique identifier only to count ad impressions, is not transferring PII to a third party, if its notice to customers and its contract with ad networks complies with the CCPA requirements. However, if the ad network retains the information or if the app developer agrees to serve behaviourally targeted advertising, that cannot be accommodated within the above provision and all the provisions of the CCPA must be complied with.

An ad network which provides false contractual representations that it does not further collect, use or disclose PII is liable for violating the CCPA, but a mobile app developer who contracted in good faith with such a network would not be liable provided the developer did not have actual knowledge or reason to believe that the ad network intended to do so.[241] The key question would be whether it was objectively reasonable for the app developer to be unaware of the ad network's intended use of the PII.

---

[239] This follows from the definition of 'third party' in §1798.140(w) as 'a person who is *not* any of the following:
(1) The business that collects personal information from consumers under this title.
(2) (A) A person to whom the business discloses a consumer's personal information for a business purpose pursuant to a written contract, provided that the contract:
(i) Prohibits the person receiving the personal information from:
  (I) Selling the personal information.
  (II) Retaining, using, or disclosing the personal information for any purpose other than for the specific purpose of performing the services specified in the contract, including retaining, using, or disclosing the personal information for a commercial purpose other than providing the services specified in the contract.
  (III) Retaining, using, or disclosing the information outside of the direct business relationship between the person and the business.
(ii) Includes a certification made by the person receiving the personal information that the person understands the restrictions in subparagraph (A) and will comply with them'.

[240] By the same reasoning, analytics companies that provide app analytics to improve app performance, but also monetise the aggregated data, may arguably be third parties.

[241] Ibid §1798.140(w)(2)(B) provides that: 'A person covered by this paragraph that violates any of the restrictions set forth in this title shall be liable for the violations. A business that discloses personal information to a person covered by this paragraph in compliance with this paragraph shall not be liable under this title if the person receiving the personal information uses it in violation of the restrictions set forth in this title, provided that, at the time of disclosing the personal information, the business *does not have actual knowledge, or reason to believe, that the person intends to commit such a violation*' (own emphasis).

(d) Data Protection Principles

The CCPA addresses many of the shortfalls of CalOPPA. First, it deals more comprehensively with the content of a privacy disclosure. A business must disclose both the categories of PII *and* the purposes for which it shall be used, before or at the time of collection.[242] If it has not sold PII or disclosed PII for business purposes, it must disclose that fact.[243] Further, a consumer must be notified of the right to request what PII has been collected about him or her, and to request the deletion of his or her PII, and of how to exercise those rights. [244]

Like CalOPPA, the CCPA requires that the privacy policy, or other disclosure notice, must be 'reasonably accessible' via a 'clear and conspicuous link',[245] and up to date.[246] The CCPA does not, however, require that steps be taken to verify that a customer has received or read the notice, or any updated terms; nor does the CCPA include the express requirements of a COPPA compliant policy that it be easy to understand and not confusing or contradictory.[247]

Provision of an online service cannot be made conditional upon the consumer agreeing to the sale of PII, and a consumer must be notified of the right to opt-out.[248] All consumers must be given 'explicit notice' if third parties will on-sell PII and must be notified of the right to opt-out.[249] A privacy policy may therefore not contain a disclaimer that customers should not use the app if they do not agree to all the terms of use. Furthermore, where the

---

[242] Ibid §1798.100(b). 'A business that collects a consumer's personal information shall, at or before the point of collection, inform consumers as to the categories of personal information to be collected and the purposes for which the categories of personal information shall be used. A business shall not collect additional categories of personal information or use personal information collected for additional purposes without providing the consumer with notice consistent with this section'. Further, §1798.130(a)(5)(B) & (C) require a business to maintain separate publicly available lists of the categories of personal information collected, sold, and disclosed for business purposes in the preceding 12 months.

[243] Ibid §1798.115(c)(1) & (2). The section is somewhat ambiguous as to whether such disclosure must always be made or only if the app may collect this information but has not yet done so. As a matter of best practice, a privacy policy should clearly state what information is not collected, sold or disclosed. See e.g. TrustArc, 'Truste Model Privacy Disclosures' <http://chnm.gmu.edu/digitalhistory/links/cached/chapter6/6_24c_disclosures.htm> accessed 3 March 2020, and Future of Privacy Forum and Center for Democracy & Technology, 'Best Practices for Mobile Application Developers' (12 July 2012) <https://fpf.org/wp-content/uploads/Apps-Best-Practices-v-beta.pdf> accessed 28 February 2020.

[244] CCPA §1798.130(a)(5)(B). Trained employees must respond to customer requests (§1798.130(a)(6)).

[245] Ibid §1798.130(a).

[246] Ibid §1798.130(a)(5) requires that it be updated at least once every 12 months. It should be updated sooner if there is a 'material change' (CalOPPA(§22575(b)(3)).

[247] COPPA Rule 16 C.F.R §312.4(a). For each material change in processing COPPA requires fresh notice and consent.

[248] CCPA §1798.105(b) read with §1798.130.

[249] Ibid §1798.115(d).

business has 'actual knowledge' that a consumer is under 16, it must first seek 'affirmative authoris[ation] to sell' (i.e. opt-in consent) from the consumer (or a parent or guardian of a child under 13).[250]

Although a business is not prohibited from incentivising voluntary disclosure of additional information by reasonable and fair means, it may not discriminate against a consumer,[251] and must obtain opt-in consent for any financial incentive scheme.[252] In addition, a business is not prohibited from asking for consent more than once, and acting upon subsequently received 'express authorisation' to sell PII,[253] but harassing or tricking a consumer into providing the consent through constant or misleading requests would be an unfair and deceptive trade practice that might attract regulatory sanction by the FTC.[254]

Secondly, the CCPA deals with customer rights, and how businesses should assist customers to exercise those rights (which is entirely absent from CalOPPA). Under the CCPA, a business must 'promptly'[255] respond to a 'verifiable consumer request'[256] to disclose the PII that the business has collected about the consumer, subject to a maximum of two requests per year.[257] When doing so, it must disclose 'the specific pieces of [PII] it has collected about that customer',[258] together with the 'categories' of PII it collects,[259] the 'categories of sources' from which it obtains PII,[260] the 'business or commercial purpose for collecting or selling the [PII]',[261] and the 'categories of third parties with whom the business shares [PII]',[262] for the preceding 12 months.[263] The response must be sufficiently detailed to make it clear which categories of PII were 'sold' (as defined) to which categories of third parties,[264] and which categories of PII were disclosed for which business purposes.[265] Upon receipt of a

---

[250] Ibid §1798.120(c). Importantly, the section provides that '[a] business that willfully disregards the consumer's age shall be deemed to have had actual knowledge of the consumer's age'.
[251] Ibid §1798.125(a).
[252] Ibid §1798.125(b). Financial incentive practices may not be 'unjust, unreasonable, coercive, or usurious'.
[253] Ibid §1798.120(d).
[254] Pursuant to its powers under s 5 of the FTCA.
[255] And within 45 days (CCPA §1798.130(a)(2) read with §1798.100(d)).
[256] ibid §1798.140(y), which provides for further regulations to be issued by the Attorney General.
[257] Ibid §§1798.100(a), (c) & (d).
[258] Ibid §1798.110(a)(5).
[259] Ibid §1798.110(a)(1).
[260] Ibid §1798.110(a)(2).
[261] Ibid §1798.110(a)(3).
[262] Ibid §1798.110(a)(4).
[263] Ibid §1798.130(a)(3)(B).
[264] Ibid §1798.115(a)(2).
[265] Ibid §1798.115(a)(3).

verified consumer request to delete PII, the business must delete all PII held on their own servers and direct service providers to do the same.[266]

Although the CCPA does not directly address data minimisation, it may indirectly encourage businesses to delete information immediately when it is required for one-time use, and to anonymise information as soon as possible, as a business is not required to respond to consumer requests in respect of such data.[267] Lawful use and retention of PII, beyond the requirements of bona fide research and compliance with legal obligations, is restricted to 'internal uses' that a customer would reasonably anticipate in the context of his or her relationship with the business.[268]

VIII CONCLUSION

The analysis of COPPA in this chapter illustrates that it sets a benchmark for robust data protection relying on verified opt-in consent from the parents of children. Further, under COPPA, CalOPPA and the CCPA, apps must have a complete and clear privacy policy, with the CCPA requiring a clear 'opt-out' mechanism from the sale of personal information. However, the statutory provisions apply to 'operators', i.e. the app developer or app owner, and do not impose direct accountability on downstream processors, or upstream technology or platform providers. In the next chapter, the position under EU law will be considered.

---

[266] Ibid §1798.105(c), provided that under subdivision (d) of §1798.105, a business or a service provider may retain PII if it is required to perform the contract, (e.g. to complete the transaction for which it was collected, for warranty and product recall purposes, or 'provide a good or service requested by the consumer, or reasonably anticipated within the context of a business' ongoing business relationship with the consumer'). It may also be retained for internal purposes such as security and debugging, free speech, public scientific, historical or statistical research or compliance with a law enforcement warrant under California Electronic Communications Privacy Act of 2015, Cal. Pen. Code §1546 (CalECPA) or another legal obligation.

[267] CCPA §1798.100(e) provides: 'This section shall not require a business to retain any personal information collected for a single, one-time transaction, if such information is not sold or retained by the business or to reidentify or otherwise link information that is not maintained in a manner that would be considered personal information'.

[268] Ibid §1798.105(d) provides:

'A business or a service provider shall not be required to comply with a consumer's request to delete the consumer's personal information if it is necessary for the business or service provider to maintain the consumer's personal information in order to …

(7) enable solely internal uses that are reasonably aligned with the expectations of the consumer based on the consumer's relationship with the business;

…

(9) otherwise use the consumer's personal information, internally, in a lawful manner that is compatible with the context in which the consumer provided the information'.

CHAPTER 5

EU DATA PROTECTION LAW

I INTRODUCTION

This chapter will examine how the principles of data minimisation and accountability, which were identified in chapter 3 as being central to an effective PbD approach, are dealt with in the EU under GDPR and the e-Privacy Directive. It will first set out the definition of key concepts, namely: personal information, the responsible party, consent (as the primary basis for lawful processing), notice, and other grounds of lawful processing. These issues were identified in chapter 3 as being central to the analysis of a PbD approach to data protection.

II THE GENERAL DATA PROTECTION REGULATION (2016) (GDPR)

(a) Origin and Background

The GDPR replaces the 1995 Data Protection Directive and became effective on 25 May 2018. Its origins lie in concerns about the effectiveness of data protection in Europe.[1] It marks a continuation of the high priority placed on the fundamental right to privacy in relation to the automatic processing of personal information.[2] However, it also records the shift to the inclusion of a separate right to data protection in the Charter of Fundamental Rights and Freedoms.[3]

While data protection in the EU is guided by the principle that the conditions under which data can be lawfully processed should be equivalent,[4] in reality there was

[1] These concerns are discussed further in chapter 8 with specific reference to privacy by design.
[2] As to which see David H. Flaherty, *Protecting Privacy in Surveillance Societies: The Federal Republic of Germany, Sweden, France, Canada, and the United States* (The University of North Carolina Press 1989) discussed in chapter 1. Also see David H Flaherty, 'On the Utility of Constitutional Rights to Privacy and Data Protection' (1990) 41 *Case W Res L Rev* 831–856.
[3] Charter of Fundamental Rights of The European Union (2000/C 364/01) art 8.
[4] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA OJ L 119, 4.5.2016 (EU General Data Protection Regulation; GDPR) rec10.

insufficient harmony between the member state laws enacted to implement the 1995 Directive.[5] As a Regulation rather than a Directive, GDPR is directly applicable in the member States, and this should lead to greater harmony as to how the core data protection principles are interpreted and applied.[6] GDPR does, however, remain a lengthy and complex instrument, comprising some 99 articles, and a further 173 recitals.[7]

Moreover, GDPR is subject to sector-specific laws, such as the e-Privacy Directive, which impose specific provisions that supplement the more general provisions of GDPR.[8] The provisions should thus be interpreted in harmony with GDPR, but in the event of a conflict, the specific provisions must prevail.[9] Member States have also enacted several sector-specific laws in areas where additional regulation is required,[10] and GDPR affords member states a margin of appreciation in a number of key respects, such as the age of consent (discussed below).

(b) Personal Information

GDPR applies to the 'processing'[11] of personal data:

> *'"personal data" means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification*

---

[5] European Data Protection Supervisor (EDPS), *Opinion of the European Data Protection Supervisor on the Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions - "A comprehensive approach on personal data protection in the European Union"* (2011) at §§49–51.

[6] Ibid at §§64–65.

[7] GDPR. The recitals are supplementary text that provide explanations which will be taken into account by the European Data Protection Board (EDPB), supervisory authorities in member States, and the Court of Justice of the European Union (CJEU) in interpreting and applying the articles of GDPR.

[8] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (e-Privacy Directive) OJ L 201/37, 31.7.2002 rec 12 and art 1(2). The provisions are meant to 'particularise and complement' the general law.

[9] European Data Protection Board, *Opinion 5/2019 on the Interplay between the ePrivacy Directive and the GDPR, in particular regarding the Competence, Tasks and Powers of Data Protection Authorities* (12 March 2019) at para 39–40. GDPR art 95 provides that processing in connection with the provision of publicly available electronic communications services in public communication networks shall not be subject to 'additional obligations' under the Regulation insofar as the e-Privacy Directive imposes 'specific obligations with the same objective'.

[10] GDPR rec 10.

[11] Ibid art 4(2). The term 'processing' is defined as 'any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.'

number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;'[12]

In this regard, GDPR, like the 1995 Directive and the Protection of Personal Information Act, uses the phrase 'related to an identified or identifiable natural person' to indicate that any information that may directly or indirectly identify a person is personal information.[13] The categories of information referred to in article 4(1) are thus not a closed list.

The terms 'identifier' and 'online identifier' are not defined, but examples that would be interpreted mutatis mutandis include a name (which, it is submitted, may be either a real name or an online alias used as a screen name or user name). The term 'any identification number' would thus not include only an identity card number, driver's licence number or account number but has been held to include an IP address, as it allows an individual to be 'precisely identified'.[14] Similarly, location data must include precise and approximate GPS location and location data inferred indirectly from, for example, Wi-Fi and Bluetooth connections. Adopting a purposive interpretation, the term 'personal data' should be interpreted widely,[15] particularly when large-scale automated processing of datasets or metadata is involved.[16]

The definition also refers to a range of factors about a person which could be used, directly or indirectly, to identify that person. A privacy policy must therefore specify if such information is processed and should pay particular attention to 'sensitive' and 'special' personal information.

---

[12] Ibid art 4(1).
[13] Article 29 Data Protection Working Party, *Opinion 4/2007 on the concept of personal data* (WP 136) at 9. Data self-evidently relates to an individual when the *content* refers to an identifiable individual, but when the content ostensibly relates to an object (such as a mobile device) it can still be considered as indirectly 'relating to' an individual when the object is linked to an individual (through ownership or proximity of location or interaction with other objects owned by the individual) with the *purpose or result* that something is revealed about the identity, characteristics or behaviour of an individual, or the information determines or influences the way in which that person is treated or evaluated.
[14] *Scarlet Extended v Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)* (C-70/10) ECLI:EU:C:2011:771 para 51 (pertaining to ISPs). Also see *Breyer* (C-582/14) ECLI:EU:C:2016:779 para 49, holding that a dynamic IP address, which changes each time there is a connection to the internet, is personal data when collected by an online media service, insofar as it had legal means to render an individual identifiable by obtaining additional data held by the internet service provider (ISP).
[15] *Lindqvist* (C-101/01) ECLI:EU:C:2003:596 para 50. As to the similar provisions in POPIA see chapter 6.
[16] *Rīgas satiksme* (C-13/16) ECLI:EU:C:2017:336 para 95.

Although the term ‘sensitive’ personal information is used in GDPR recitals 10 and 51 as synonymous with the categories of ‘special personal data’ defined in article 9(1), the two terms should be distinguished.

Article 9(1) contains a limited set of categories of ‘special’ personal information.[17] Recital 51 records that such details are ‘by their nature, particularly sensitive in relation to fundamental rights and freedoms and merit specific protection as the context of their processing could create significant risks to the fundamental rights and freedoms’. There is a general prohibition against processing special personal information without the data subject’s ‘explicit consent’.[18]

GDPR expressly includes ‘genetic’[19] and ‘biometric’[20] information as ‘special’ personal information, making it clear that processing these categories of information requires additional safeguards alongside health information. [21] GDPR also includes information that reveals racial and ethnic origin[22] as special personal information. Although photographs may indirectly reveal such information, they are not included, save to the extent that facial recognition, or other biometric access controls, is used.[23]

Although the term ‘sensitive’ information[24] is used by industry and regulatory guidance in the US in a roughly equivalent sense in relation to health information, and

---

[17] GDPR art 9(1) reads: ‘Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited’.

[18] Ibid art 9(2)(a), with the proviso that member State laws may stipulate that data subjects cannot consent to the processing of special personal information, and the further provision under art 9(4) for State laws controlling or limiting the processing of genetic, biometric or health information.

[19] Ibid art 4(13). '[G]enetic data' is defined as ‘personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question’.

[20] Ibid art 4(14). ‘[B]iometric data' is defined as ‘personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data’.

[21] Ibid art 4(15). '[D]ata concerning health' is defined as ‘personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status’.

[22] The term is not defined. Recital 51 expressly disclaims implication that the EU accepts ‘theories which attempt to determine the existence of separate human races’.

[23] Recital 51 expressly records that ‘the processing of photographs should not systematically be considered to be processing of special categories of personal data as they are covered by the definition of biometric data only when processed through a specific technical means allowing the unique identification or authentication of a natural person’.

[24] As explained in chapter 2, in relation to mobile applications, the term has its origins in the varying classifications of certain permissions as ‘sensitive’ or ‘dangerous’ by OS platforms.

information about a person's political, religious or sexual preferences, it also encompasses inter alia location information,[25] financial information[26] and children's information.[27] While such data are not included in article 9, they are still personal information and processing such information may carry a 'high risk to the fundamental rights and freedoms of the data subject'.[28] Sensitive data in this context would include information linked to the highly private aspects of personal and home life, but may extend beyond strictly private or confidential information to include information that could infringe other rights or cause serious harm to the data subject's interests.[29]

Thus, as in the US, additional safeguards need to be considered when processing these types of information. The collection of location (and other information) for the purposes of targeted advertising, or credit scoring, for example, falls within the definition of 'profiling'[30] and requires disclosure,[31] data subject access to the records,[32] 'explicit consent' for such

[25] The term is not defined. See discussion above of its express inclusion as 'personal information'. Information about a person's location or movements that is used to infer, e.g. political or religious affiliations, would need to be treated as 'special personal information'.
[26] The term is not defined. Financial information must reveal the identity of a person to be 'personal information'. Financial information used to infer, e.g. political or religious affiliations from payments made or received, would need to be treated as 'special personal information'.
[27] GDPR art 8 contains specific provisions relating to children.
[28] In terms of art 35(1). See Article 29 Data Protection Working Party, *Guidelines on Data Protection Impact Assessment (DPIA) and Determining Whether Processing is "Likely to Result in a High Risk" for the Purposes of Regulation 2016/679* (WP 248 rev01, 4 April 2017, last revised October 2017) at 9.
[29] Ibid. 'Sensitive' data is described in the report as 'data linked to household and private activities (such as electronic communications whose confidentiality should be protected), or because they impact the exercise of a fundamental right (such as location data whose collection questions the freedom of movement) or because their violation clearly involves serious impacts in the data subject's daily life (such as financial data that might be used for payment fraud). … This criterion may also include data such as personal documents, emails, diaries, notes from e-readers equipped with note-taking features, and very personal information contained in life-logging applications'.
[30] GDPR art 4(4). The term 'profiling' is defined as 'any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements'.
[31] Ibid art 13(2)(f) and 14(2)(g). Although this will be difficult where complex algorithms and internal processes are used, GDPR requires that the data subject be given 'meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.'
[32] Ibid art 15(1)(h).

practices,[33] and the application of technical and organisational measures to ensure fairness to the data subject.[34]

The personal information of children requires 'specific protection',[35] on the grounds that they may not appreciate the privacy risks nor understand their rights and the safeguards available to protect their privacy. Although article 8 applies to any offer of 'information society services directly to a child',[36] the interpretative guidance contained in recital 38 draws particular attention to marketing aimed at children, and building profiles of children, such as a personality profile or user profile.

Where the controller relies on consent for the lawfulness of processing the personal information of a child,[37] it must obtain verified parental consent.[38] GDPR regards a person under 16 as a child,[39] although member States may provide an age of consent from 13, and the age of consent thus varies from 13 to 16 across the EU. [40]

---

[33] Ibid art 22. Subject to law and the data subject's right to object, explicit consent is not required if processing is necessary for performing the contract.
'1. The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.
2. Paragraph 1 shall not apply if the decision:
(a) is necessary for entering into, or performance of, a contract between the data subject and a data controller;
(b) is authorised by Union or Member State law to which the controller is subject, and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or
(c) is based on the data subject's explicit consent'.

[34] Ibid art 5(1)(a) imposes a general obligation on the controller to ensure that processing is both lawful and fair. Art 22(3) states that 'the data controller shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision'. See further rec 71–73.

[35] Ibid rec 38.

[36] The requirement in GDPR for an offer 'directly' to a child (as opposed to a broader service that may indirectly be used or viewed by children, is similar to the scope of COPPA that applies when the website or online service is 'directed at' children.

[37] Ibid art 8(1). 'Where point (a) of Article 6(1) applies, in relation to the offer of information society services directly to a child, the processing of the personal data of a child shall be lawful where the child is at least 16 years old. Where the child is below the age of 16 years, such processing shall be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child'.

[38] Ibid art 8(2). 'The controller shall make reasonable efforts to verify in such cases that consent is given or authorised by the holder of parental responsibility over the child, taking into consideration available technology.' This is comparable to the requirements of Children's Online Privacy Protection Rule, 16 C.F.R part 312 (COPPA Rule).5(b), discussed in chapter 4.
Although the European Data Protection Board (EDPB) is not empowered under art 70 to stipulate methods for obtaining consent, the compliance methods approved by the FTC could be referred to as best practice guidelines, or included in industry codes, and certification programs submitted to the EDPB for approval under art 70(1)(n) read with art 40(2)(g).

[39] GDPR art 8(1).

[40] Ibid. As at 1 July 2019 the age of consent is 13 in Belgium, Denmark, Estonia, Finland, Latvia, Malta, Portugal, Sweden and the United Kingdom. The age of consent is 14 in Austria, Bulgaria, Cyprus, Italy, Lithuania and

Publicly available information is not expressly excluded from the definition of 'personal information', although the fact that it has 'deliberately' been made public would normally indicate that the data subject has waived any privacy interest,[41] and may indicate that the processing is not 'high risk'.[42]

Personal information does not include anonymous data, that is to say, data which cannot be used to identify a person by means of techniques 'reasonably likely' to be used (taking into account the cost, time and current available technology).[43] GDPR does not apply to anonymous data, which can be used for any statistical or research purposes.[44] GDPR distinguishes anonymous data from pseudonymous data, where the data set is stripped of identifiers, but remains capable of being re-identified if combined with additional information. Article 4(5) provides:

> *'pseudonymisation' means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;'.*

Technical measures to retain separate databases, and organisational measures to restrict which persons are authorised to access each database, would be used to prevent the reversal of pseudonymisation, and in this way, the risk to the data subject, if there was a data

---

Spain. The age of consent is 15 in Czech Republic and France and has been included in draft legislation in Greece and Slovenia. See Ingrida Milkaite and Eva Lievens, 'The GDPR child's age of consent for data processing across the EU – one year later (July 2019)' (1 July 2019) <https://www.betterinternetforkids.eu/web/portal/practice/awareness/detail?articleId=3017751> accessed 22 August 2019.

[41] GDPR art 9(e). Processing 'special' personal information is not prohibited where the information has been 'manifestly made public by the data subject'.

[42] Article 29 Data Protection Working Party, *Guidelines on Data Protection Impact Assessment (DPIA) and Determining Whether Processing is "Likely to Result in a High Risk" for the Purposes of Regulation 2016/679* at 9 explains that where data has been made publicly available by the data subject (or by a third party) this may indicate that further processing is reasonably anticipated.

[43] GDPR rec 26 records 'To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments'.

[44] Ibid rec 26 continues 'The principles of data protection should therefore not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable. This Regulation does not therefore concern the processing of such anonymous information, including for statistical or research purposes.'

breach, is minimised. Pseudonymised data remains subject to GDPR, although the notice and storage limitations are relaxed for 'archiving in the public interest, statistical, historical or scientific research'.[45]

(c) Controller

The 'controller' is 'the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data'.[46]

There can thus be more than one controller. They could act as joint controllers in respect of the same processing. However, the definition does not preclude the possibility of multiple controllers each separately processing the same information for their own purposes.

A controller established in the EU must comply with GDPR in respect of all processing (even of non-EU residents' personal information), regardless of where the processing takes place.[47]

A mobile application developer is a controller. They fall squarely within the ambit of the defination in article 4(7) as they determine the "purposes and means" by which the app processes personal information. A South African mobile app developer that has an 'establishment'[48] in the EU can take advantage of the rationalising provisions that provide for regulatory and legal actions to be pursued in the Member State where it has its main establishment in the EU.[49] However, they would then have to ensure that they process all

---

[45] Ibid art 5(1)(b) provides that 'further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes'. Art 89(1), read with rec 156, requires such processing to be subject to 'appropriate safeguards' and in accordance with the principle of data minimisation. The controller must anonymise the data, unless this is not feasible, in which case appropriate safeguards should be applied such as pseudonymising the data.

[46] Ibid art 4(7). EU or Member State laws may further regulate the specific criteria applicable in a particular context.

[47] Ibid art 3(1). 'This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.'

[48] The term is not defined. Rec 22 provides that '[e]stablishment implies the effective and real exercise of activity through stable arrangements. The legal form of such arrangements, whether through a branch or a subsidiary with a legal personality, is not the determining factor in that respect'.

[49] GDPR art 56(1) means that where a controller has an establishment in the EU in most cases, subject to art 56(2), multiple complaints will be consolidated under one investigation by the 'leading supervisory authority' where the controller has its main establishment.

personal information in accordance with GDPR where this imposes a higher standard than the Protection of Personal Information Act.[50]

A controller established outside the EU must comply with GDPR insofar as it processes the personal data of EU residents.[51] The determination of whether a mobile app developer is offering services to EU residents requires consideration as to whether it 'is apparent that the controller or processor envisages offering services to data subjects in one or more Member States in the Union'.[52] This may appear from factors such as the language or currency settings of the app,[53] reference to EU users (for example, in the app's privacy policy or marketing statements),[54] and regional restrictions.[55]

Thus a South African app developer whose app is made available for download by EU residents[56] would be subject to GDPR, regardless of where the app developer is established, and liable for the regulatory measures[57] and large fines,[58] and faced with the

---

[50] GDPR art 79(2). 'Proceedings against a controller or a processor shall be brought before the courts of the Member State where the controller or processor has an establishment. Alternatively, such proceedings may be brought before the courts of the Member State where the data subject has his or her habitual residence, unless the controller or processor is a public authority of a Member State acting in the exercise of its public powers.'

[51] GDPR art 3(2). 'This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:

(a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or

(b) the monitoring of their behaviour as far as their behaviour takes place within the Union.'

[52] Ibid rec 23.

[53] Ibid rec 23. If the app settings permit users to select a European language, or to make in-app purchases in Euro, this would be a clear indication that the app developer envisages offering the app to EU residents and must therefore comply with GDPR.

[54] Ibid rec 23.

[55] Apps can be 'region-locked' and cannot be downloaded if the geographical location registered to the device falls outside that region. Users can by-pass this restriction by resetting their iTunes or Google Play store location. See e.g. Amboy Manolo, 'Change Your App Store Country to Download Region-Locked Apps & Games on Your iPhone' (21 March 2017) <https://ios.gadgethacks.com/how-to/change-your-app-store-country-download-region-locked-apps-games-your-iphone-0176591/> accessed 13 March 2020 and 'Downloading Region Restricted Apps on Android' (1 March 2019) <https://hide.me/en/knowledgebase/downloading-region-restricted-apps-on-android/> accessed 13 March 2020.

[56] If the app is region-locked but EU residents bypass these settings, it is submitted that the app developer still needs to comply with GDPR if it acquires actual knowledge that EU residents have downloaded its app and it takes no steps to close those accounts.

[57] GDPR art 58.

[58] Ibid art 83. In terms of art 83(5) infringement of the basic conditions of processing (e.g. consent), a data subject's rights or cross-border transfers of personal information without lawful safeguards is subject to a maximum fine of EUR 20 million, or (in the case of an 'undertaking') 4% of annual turnover worldwide in the preceding financial year, whichever is higher. Where a mobile app developer is part of a group of companies (such as a South African subsidiary of a multi-national software company) each company in the group would constitute an undertaking and the fine might be based on group revenue. (GDPR does not define the term 'undertaking', but rec 150 requires the term to be used consistent with art 101 and art 102 of the Treaty on the Functioning of the

spectre of multiple data protection investigations,[59] and civil actions in the member States where each data subject is habitually resident.[60]

Parties are 'joint controllers' where 'two or more controllers jointly determine the purposes and means of processing'.[61] GDPR requires that they implement an 'arrangement' that determines their respective responsibilities in a transparent manner (and may designate a single contact point for data subjects).[62] GDPR is otherwise silent about the allocation of accountability between controllers.[63]

A controller may use one or more 'processors'[64] to carry out all or part of the processing on its behalf. Where the controller uses a processor to process data on its behalf, this must take place in accordance with a comprehensive contract.[65] The contract must require the processor to act only on 'documented instructions' from the controller.[66] A processor must be required to notify the controller before appointing a sub-processor,[67] and before transferring data to a third country (that is, one outside the EU),[68] and must guarantee implementation of appropriate security safeguards.[69] If the processor makes further use of the information, it not only acts in breach of the contract, but is regarded as a controller in its own right for the

European Union (TFEU) (Treaty of Lisbon) (13 December 2007) – a discussion of the case law related to groups is beyond the scope of this dissertation which focuses on the position of small mobile app developers.

[59] GDPR art 77(1) gives a data subject the right to lodge a complaint with a data supervision authority in the Member State where the data subject habitually resides, or works, or where the infringement took place. Where a controller does not have any establishment in the EU, there is no 'lead supervisory authority' and the data protection authority in each Member State where a compliant is laid would conduct its own investigation.

[60] GDPR art 79(2).

[61] GDPR art 26(1).

[62] Ibid.

[63] The Article 29 Working Party opines that to rely on consent, all joint controllers must be named in the disclosure notice (whereas processors do not need to be named, provided the type of processor is included in the categories of recipients to whom data will be transferred). Article 29 Data Protection Working Party, *Guidelines on Consent under Regulation 2016/679* (WP 259, 28 November 2017) at 13.

[64] GDPR art 4(8). The term 'processor' is defined as 'a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller'.

[65] Ibid art 28(3)(a)-(h). The contract must record the subject matter of the processing, including the types of personal information, categories of data subject, and purpose and duration of processing.

[66] Ibid art 28(3)(a).

[67] Ibid art 28(2) & 28(3)(d).

[68] Ibid.

[69] Ibid art 28(1), 28(3)(d) & art 32. These include technical measures, such as encryption and pseudonymisation of data, and organisational measures, such as confidentiality guarantees from the natural persons under their authority who have access to the data.

purposes of GDPR.[70] Both parties would be liable to pay compensation to the data subject(s) for any harm suffered,[71] and would be liable for administrative fines[72] and penalties.[73]

This places an onerous contractual burden on controllers to ensure that adequate contractual safeguards are implemented. This can be fulfilled by relying in whole or in part on standard clauses,[74] and in January 2020, the EDPB published the standard form contract adopted by the Danish Data Protection Authority.[75]

In the context of mobile apps, the developer may contract with multiple processors to provide backend services and data storage salutation. The standard contract can be used for contract negotiations, and even in situations where large processors present 'take it or leave it' standard terms and conditions, the standard contract provides a useful reference to determine if those conditions are GDPR compliant.

A controller can also disclose personal information to a 'third party',[76] that is to say, a person who will process it without acting under the controller's authority, provided the controller acts lawfully in disclosing the information on the basis of the data subject's consent, or some other ground of lawful processing. The person who receives the information will be a

---

[70] Ibid art 28(10). 'Without prejudice to Articles 82, 83 and 84, if a processor infringes this Regulation by determining the purposes and means of processing, the processor shall be considered to be a controller in respect of that processing'.

[71] Ibid art 82(4), save if they can demonstrate they were 'in no way responsible for the event' (in terms of art 82(3)).

[72] Ibid art 83, although the amount of the fine would take into consideration, inter alia, whether the infringement was intention or negligent pursuant to art 83(2)(d).

[73] Ibid art 84.

[74] Ibid art 28(6). Under art 28(8) a supervisory authority may adopt standard contractual clauses, and these can be reviewed by the EDPB in terms of the consistency mechanism under art 63. As to the approved content of such standard contractual clauses under the 1995 Data Protection Directive see Commission Decision (EU) no 2004/915/EC of 27 December 2004 amending Decision 2001/497/EC as regards the introduction of an alternative set of standard contractual clauses for the transfer of personal data to third countries (notified under document number C(2004) 5271) (Text with EEA relevance) OJ L 385, 29.12.2004. After this thesis was submitted for examination a proposal to revise this decision pursuant to GDPR was put forward. See Draft Commission Implenting Decision (EU) on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council Ref: Ares(2020)6654686, 12.11.2020.

[75] Datatilsynet (Danish Data Protection Agency), *DK SA Standard Contractual Clauses for the Purposes of Compliance with Art. 28 GDPR* (2019). Also see European Data Protection Board, *Opinion 14/2019 on the draft Standard Contractual Clauses submitted by the DK SA (Article 28(8) GDPR)* (2019). As the first of its kind the document is instructive as to the wording of such contracts.

[76] GDPR art 4(10). The term 'third party' is defined as 'a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data'.

'recipient',[77] but could be regarded as a controller in his or her own right if they 'determine the means and purpose of processing' the information. For example, a third party ad network would meet the definition of a controller as (acting with publishers and advertisers) they determine the purpose and means of processing through the code contained in the ad library. It may be appropriate to regard the app developer and the ad library as joint controllers, but as indicated above, this would require a transparent arrangement between them. As explained in chapter 2, academic and industry opinion has pointed to the complete lack of transparency by aggregation platforms and ad networks about how they process data. At the same time, one cannot discount the importance of advertising as a form of revenue for app developers, nor the benefits consumers derive from free services, in exchange for advertising. GDPR's approach to the complexity of modern data-processing operations is to rely in analysis of the risk in any particular case to determine what appropriate safeguards are required.[78]

Where the processing is 'likely to pose a high risk to the rights and freedoms of natural persons' a data protection impact assessment (DPIA) must be completed by the controller before the processing starts.[79] Pursuant to article 35(4), supervisory authorities must maintain lists of such activities, and several have already done so.[80] These lists are intended to expand upon the three indicative examples of high-risk processing set out in article 35(3), namely: [81]

---

[77] Ibid art 4(9). A recipient includes any natural or legal person, but excludes public authorities processing personal information under EU or Member State law.

[78] For a fuller discussion of the risk-based approach in GDPR and how it can be reconciled with the 'rights-based' data protection principles contained in art 5, see Raphael Geller, 'We Have Always Managed Risks in Data Protection Law: Understanding the Similarities and Differences between the Rights-based and the Risk-based Approaches to Data Protection' (2016) 2 (4) *European Data Protection Law Review* 481–492 and Article 29 Data Protection Working Party, *Statement on the Role of a Risk-based Approach in Data Protection Legal Framework* (WP 218, 30 May 2014).

[79] Ibid art 35(1).

[80] The lists published by the supervisory authorities in Bulgaria, Italy, Germany, Malta, Romania, France, Ireland, United Kingdom, Slovenia, Belgium, Hungary, Czech Republic, Liechtenstein, Luxembourg, Slovakia, Latvia, Lithuania, Norway, Iceland, Poland, Croatia, and Estonia, and the 'whitelist' of exempt processing activities in France, alongside the EDPB opinions, have been published in European Data Protection Board, 'Register for Decisions taken by supervisory authorities and courts on issues handled in the consistency mechanism' <Register for Decisions taken by supervisory authorities and courts on issues handled in the consistency mechanism> accessed 19 March 2020. Although one would expect a high degree of consistency, each list is quite varied, so that careful scrutiny of the examples and explanations provided by the supervisory authorities in each particular Member State remains essential despite the consistency mechanism introduced under GDPR.

[81] Article 29 Data Protection Working Party, *Guidelines on Data Protection Impact Assessment (DPIA) and Determining Whether Processing is "Likely to Result in a High Risk" for the Purposes of Regulation 2016/679* at 9, reiterates that art 35(3) uses the words 'in particular'; thus the examples given are not a closed list.

a) Profiling: evaluation of natural persons using systematic, large scale automated processing, which produces legal effects or otherwise significantly affects the person;

b) Large scale processing of 'special' personal information or criminal convictions; and

c) Systematic monitoring of publicly-accessible areas on a large scale.[82]

The Article 29 Working Party guidelines suggest nine additional risk criteria, which are in turn broadly reflected in the country lists:[83]

1. 'Evaluation or scoring, including profiling and predicting;'[84]
2. 'Automated-decision making with legal or similar significant effect;'[85]
3. 'Systematic monitoring;'[86]
4. 'Sensitive data or data of a highly personal nature;'[87]
5. 'Data processed on a large scale;'[88]

---

[82] GDPR art 35(3).

[83] Article 29 Data Protection Working Party, *Guidelines on Data Protection Impact Assessment (DPIA) and Determining Whether Processing is "Likely to Result in a High Risk" for the Purposes of Regulation 2016/679* at 9–11.

[84] Ibid. Drawing on rec 71 & 91, a data subject's 'work performance, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements' merit special attention (recitals 71 and 91). E.g. banks or insurers conducting credit and fraud screening; biotech's offering genetic (or health screening) or the creation of 'behavioural or marketing profiles' based on website visits.

[85] Ibid. Drawing on art 35(3)(a), this includes any processing that 'may lead to the exclusion or discrimination against individuals'. See further Article 29 Data Protection Working Party, *Guidelines on Automated Individual Decision-making and Profiling for the Purposes of Regulation 2016/679* (WP251, rev01, 3 October 2017, last revised 6 February 2018).

[86] Article 29 Data Protection Working Party, *Guidelines on Data Protection Impact Assessment (DPIA) and Determining Whether Processing is "Likely to Result in a High Risk" for the Purposes of Regulation 2016/679* at 10. Drawing on art 35(3)(c), this includes 'monitoring' of 'data collected through networks' which, it is submitted, must include content, traffic and location data of electronic communications and networks. E.g. 'large-scale and/or systematic processing of telephony, Internet or other communication data, metadata or location data of natural persons' use to track natural persons (when not strictly necessary for the service) including monitoring public transport.

[87] Ibid. This is broader than 'special' data under art 9 and criminal records under art 10 and includes all 'sensitive' data as commonly understood to include location data, financial data, and private communications.

[88] Although it may be thought that it would be particularly helpful, especially for small enterprises, to define 'large scale processing' by reference to specific criteria, there is no definition in GDPR. Article 29 Data Protection Working Party, *Guidelines on Data Protection Officers ('DPOs')* (WP 243 rev01, 13 December 2016, last revised 5 April 2017) at 21 provides these criteria: '(a) the number of data subjects concerned, either as a specific number or as a proportion of the relevant population; (b) the volume of data and/or the range of different data items being processed; (c) the duration, or permanence, of the data processing activity; and (d) the geographical extent of the processing activity'. The Czech Republic (noting the EDPB requirement to leave out explicit figures) nevertheless provides as guidance that large scale includes more than 10000 data subjects or more than 1,0 % of the population of the State where processing is taking place, as well as 20 or more employees and/or locations where processing

6. ‘Matching or combining datasets;’[89]
7. ‘Data concerning vulnerable data subjects,’ such as children;[90]
8. ‘Innovative use or applying new technological or organisational solutions;’[91] and
9. ‘Denial of rights or services’.[92]

The guidelines propose that where two or more risk criteria are present, the processing is ‘high risk’, although each controller must carry out a case-by-case assessment, as in a particular case, any one criterion, or other unlisted criteria, may justify treating the processing as ‘high risk’.[93]

Advertising, and aggregation by analytics and social networking platforms, would easily meet these criteria, but there is considerable scope for flexibility in how the provisions relating to high-risk processing will be interpreted and applied by national supervisory authorities.

(d) Data Protection Principles

Chapter II sets out the data protection principles applicable to the processing of personal information, and chapter III sets out the rights of the data subject. GDPR articulates a broad set of data protection principles, which are fundamental to the EU approach to data protection.

---

occurs. Office for Personal Data Protection of the Czech Republic (UOOU), *List of Processing Operations Subject to Data Protection Impact Assessment* (2019) and European Data Protection Board, *Opinion 4/2018 on the draft List of the Competent Supervisory Authority of Czech Republic regarding the Processing Operations subject to the Requirement of a Data Protection Impact Assessment (Article 35.4 GDPR)* (2018).

[89] Article 29 Data Protection Working Party, *Guidelines on Data Protection Impact Assessment (DPIA) and Determining Whether Processing is “Likely to Result in a High Risk” for the Purposes of Regulation 2016/679*. The guideline restricts this to situations where the data sets arise from two or more processing operations, ‘for different purposes and/or by different data controllers in a way that would exceed the reasonable expectations of the data subject’.

[90] Ibid. Drawing on rec 75, the guiding principle put forward by the Article 29 Working Party is the existence of a ‘power imbalance’ between controller and data subject, and the guideline indicates that children ‘may be vulnerable’. This is an area of considerable divergence between country lists, both as to how children’s data is treated, and as to other vulnerable groups. E.g. the mentally ill, the elderly, and employees.

[91] Ibid. Use of artificial intelligence (AI) and internet-of-things applications (e.g. smart meters and smart TVs) would fall into this category.

[92] Ibid. See further GDPR art 22, read with rec 91.

[93] E.g. Information Commissioner's Office (UK), *Examples of Processing “Likely to Result in High Risk”* (2019) includes ‘invisible processing’ to describe situations where data is collected from sources other than the data subject and the controller determines, pursuant to art 14(5)(b), that it is impossible or would involve ‘disproportionate effort’ to give notice to the data subject.

'Article 5 Principles relating to processing of personal data

1. *Personal data shall be:*

   (a) *processed lawfully, fairly and in a transparent manner in relation to the data subject ("lawfulness, fairness and transparency");*

   (b) *collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ("purpose limitation");*

   (c) *adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ("data minimisation");*

   (d) *accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ("accuracy");*

   (e) *kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ("storage limitation");*

   (f) *processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ("integrity and confidentiality").*

2. *The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ("accountability").'*

These principles are based upon the principles set out in the COE Convention 108,[94] although GDPR has gone beyond those principles by introducing additional data subject rights, such as the right to be forgotten.[95]

Since the FIPPS of notice, consent, access and security share their origins in the same data protection principles, there are several points of overlap between US and EU data protection law. However, GDPR goes beyond the protections afforded by FIPPS under US data protection law in several key respects. COPPA, CalOPPA, and the CCPA all require that conspicuous notice be given of what personal information is collected. COPPA affords the most stringent protection in that direct notice must be given to a child's parents (for example, by email, and not simply by making a link to a privacy policy available on a website or in app settings) before the operator of a child-directed website or online service can collect any information about that child. [96] The notice must be clear and complete, and parents must be given the right to refuse to consent to the collection for processing that goes beyond the purpose of the service (for example, targeted advertising).[97] If verified parental consent[98] is not received, the contact information collected to send the notice must be deleted and no further processing of that child's information can take place. This is an opt-in consent mechanism. CalOPPA and the CCPA generally permit what is termed opt-out consent. They require that a privacy policy (or notice) be conspicuously posted describing what personal information is collected,[99] but use of the service implies that the user consents to the operator's terms and conditions.[100]

---

[94] COE Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data ETS 108 (1981, as amended in 1999), as amended by Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding supervisory authorities and transborder data flows (entry into force 1 July 2004) ETS 181 (2001) and Council of Europe Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, CETS 223 (2018) (COE Convention 108).

[95] GDPR art 17. This article goes beyond the principles of data subject participation set out in the OECD Guidelines, discussed in chapter 3. Although the controller must still delete personal data upon a request by the data subject, deletion is no longer contingent upon such a request being received. The controller must delete personal data independently and 'without undue delay' once it is no longer necessary for the purpose for which it was collected, or when there is no longer a lawful ground for processing it (as detailed in art 17(1)(a)–(f)).

[96] COPPA Rule 16 C.F.R §312.5(a)(1). Fresh notice is required when there is any 'material change' in practices.

[97] Ibid §312.5(a)(2).

[98] Ibid §312.5(b)(1).

[99] CCPA requires further that the notice clearly detail what each category of personal information is used for, and with which categories of service providers and third parties it is shared.

[100] CCPA stipulates that a user must be permitted to opt out of targeted advertising and continue to use the website and online service, but requires opt-in consent only for targeted advertising directed at children under 16 (with parental consent for children under 13).

In contrast, when consent is relied upon as the basis for processing personal information, GDPR recognises only opt-in consent as valid for all users, including children. Although it is possible to process personal data on other grounds (that is, without opt-in consent),[101] even in respect of children,[102] notice must always be given in accordance with the principle of transparency.[103] For the purposes of detailed comparison the provisions of GDPR for notice and consent will now be examined.

(i) Consent

In terms of article 6(1), where consent is relied on for processing, it is lawful 'only if and to the extent that … *(a)* the data subject has given consent to the processing of his or her personal data for one or more specific purposes'. Although GDPR does not expressly state that consent must be given before any information is collected, this is implied from the use of the past tense.[104]

Consent is defined in article 4(11) as:

> *'any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;'*

In addition, processing of special categories of personal information requires 'explicit consent'.[105]

---

[101] GDPR art 6(1) provides for 5 other grounds for processing personal information besides consent.
[102] Article 8, which details the conditions for consent to the processing of personal information of children, is invoked only '[w]here point (a) of Article 6(1) applies, in relation to the offer of information society services directly to a child'.
[103] GDPR chapter III section 1 (transparency and modalities).
[104] Further in terms of art 7(1)(a) processing is only lawful if the controller can demonstrate that the data subject 'has consented'. Arguably the past tense implies prior consent before any processing takes place. Processing, as defined in art 4(2) is 'any operation or set of operations which is performed on personal data' including collection. Also see Article 29 Data Protection Working Party, *Guidelines on Consent under Regulation 2016/679*at 17.
[105] GDPR art 9(2)(a) permits the processing of 'special' personal information despite the general prohibition in art 9(1) where 'the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject'. 'Explicit' consent therefore appears to require that in addition to an affirmative act, the consent must be given separately for a clear, separate request to collect the specified special information in respect of a clearly explained and specific purpose. However, additional grounds for lawful processing are set out in art 9(1)(b)-(j).

Thus GDPR retains the well-established requirements of the 1995 Data Protection Directive that consent must be free, specific, informed and unambiguous,[106] and that 'explicit' consent is required for processing 'special' personal information.[107]

GDPR expressly provides that the controller must be able to demonstrate that consent was given,[108] and that a request for consent must be distinguishable (that is, separate from other matters such as payment and licence terms), easily accessible, and written in clear, plain, intelligible language.[109]

Arguably, these were always implied conditions in order to meet the requirement that consent be free, specific, informed and unambiguous, but GDPR places the matter beyond doubt. Furthermore, it now provides that a data subject may withdraw his or her consent at any time, and that it must be as easy to withdraw consent as it is to give it.[110]

By definition, consent is not unambiguous unless it is contained in 'a statement or a clear affirmative act'.[111] A 'statement' is a declaration by the user which indicates by its terms that they agree to the processing.[112] A 'clear affirmative act' requires that the user takes some action from which it can be inferred that he or she intends to indicate agreement.[113] This

---

[106] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (Data Protection Directive) OJ 1995 L 281/31, 23.11.1995.
Art 2(h) defined 'the data subject's consent' as 'any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed'.
Art 7 reads: 'Member States shall provide that personal data may be processed only if: (a) the data subject has unambiguously given his consent; …'.
Art 7(b)–(f) provide alternative grounds for lawful processing that are in all material respects the same as GDPR art 6(1)(b)–(f).
[107] Ibid art 8(2)(a).
[108] GDPR art 7(1). 'Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data.'
[109] Ibid art 7(2). 'If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of such a declaration which constitutes an infringement of this Regulation shall not be binding.'
[110] Ibid art 7(3). 'The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw consent as to give it.' There was no equivalent provision in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (Data Protection Directive) OJ 1995 L 281/31, 23.11.1995.
[111] GDPR art 4(11).
[112] Ibid rec 32 indicates that a statement can be in writing, including electronic form, or oral.
[113] Ibid. Rec 32 provides the following examples: 'ticking a box when visiting an internet website, choosing technical settings for information society services or another statement or conduct which clearly indicates in this

requirement can be met only by opt-in consent.[114] Arguably, this was previously implied by the requirement under the 1995 Data Protection Directive for consent to be an 'indication' by which the data subjects 'signified' their agreement,[115] which had to be 'unambiguously given'.[116] On this basis, the CJEU held that a pre-ticked box was not valid consent for the purposes of the e-Privacy Directive.[117]

GDPR has clarified but not fundamentally altered this position,[118] although it is intended to remove the possibility for ambiguity which is heightened in an online environment,[119] and the different interpretations applied in Member State law under the Directive.[120]

Further, 'broad' or 'blanket' consent is not permissible under GDPR,[121] and a similar position had been implied under the 1995 Data Protection Directive by virtue of the requirement for a specified purpose, which was not met by accepting the general terms and conditions,[122] a pre-ticked box,[123] or the incorporation by reference to purposes set out in another contract.[124] The 'exact purpose' for which consent is given must be specified.[125]

---

context the data subject's acceptance of the proposed processing of his or her personal data. Silence, pre-ticked boxes or inactivity should not therefore constitute consent.'

[114] *Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband e.V. v Planet49 GmbH* [GC] (C-673/17) ECLI:EU:C:2019:801 at para 52–55.

[115] Data Protection Directive 95/46/EC art 2(h).

[116] Ibid art 7(a).

[117] *Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband e.V. v Planet49 GmbH* at para 52 and 55-59. At the time relevant to the decision the definition of consent in the e-Privacy Directive referred to the definition in Directive 95/46/EU.

[118] Article 29 Data Protection Working Party, *Opinion 15/2011 on the Definition of Consent* (WP187, 13 July 2011) at 11. Also see Article 29 Data Protection Working Party, *Guidelines on Consent under Regulation 2016/679* at 3–4. There have been changes but 'most of the key elements remain the same'. Further, see European Commission, *Commission Staff Working Paper Impact Assessment* (SEC(2012) 72 final, 2012) at 105.

[119] European Commission, *Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the regions: "A Comprehensive Approach on Data Protection in the European Union"* (COM(2010) 609 final) at 9.

[120] Ibid at 8.

[121] GDPR art 6(1)(a) expressly states that consent is 'for one or more specific purposes.'

[122] Article 29 Data Protection Working Party, *Working Party 29 Opinion on the Use of Location Data with a View to Providing Value Added Services* (WP 115, 25 November 2005) at 5 (in relation to article 2(h) of the Data Protection Directive 95/46/EC).

[123] Article 29 Data Protection Working Party, *Opinion 5/2004 on Unsolicited Communications for Marketing Purposes under Article 13 of Directive 2002/58/EC* (WP 90, 27 February 2004) at 5.

[124] *Pfeiffer, Roith, Süß, Winter, Nestvogel, Zeller, Döbele* [GC] (C-397/01 to C-403/01) ECLI:EU:C:2004:584 at para 85. The case concerned the definition of consent in Council Directive 93/104/EC of 23 November 1993 concerning certain aspects of the organization of working time OJ L 307, 13.12.1993.

[125] Article 29 Data Protection Working Party, *Opinion 15/2011 on the Definition of Consent* at 17.

GDPR does not contain an absolute requirement that there must be an opt-out from the collection or processing of personal information in respect of third-party data sharing.[126] However, the Article 29 Working Party has always recommended that 'granular' opt-in choices be offered where appropriate for different purposes of processing,[127] on the basis that this is required to fulfil the requirement that consent be specific and informed, and because 'bundled' consent cannot be regarded as freely given.

GDPR requires that controllers make it clear when the collection of personal data is required for the service,[128] and recital 42 provides that '[c]onsent should not be regarded as freely given if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment'. The concept of detriment is wide and includes any cost or clear disadvantage to refusing or withdrawing consent and any deception, intimidation or coercion to obtain consent.[129] For example, an app may request permission to access device accelerometer data that is not necessary for the app to function but provides useful behavioural insights for the developer about its app users' movements and activity levels (personal information). If the full functionality of the app is not available once this permission is withdrawn, this is a clear example of 'detriment' that vitiates the consent. In fact, although the user learns of the detriment only after withdrawing permission, the consent was never valid, and the accelerometer data was unlawfully collected and must be deleted.[130]

Whether compulsory third-party sharing vitiates the voluntariness of any consent given will thus depend on the facts of each case. Recital 43 records a presumption that consent is not freely given if it was 'appropriate in the individual case' to allow separate consent for different types of processing, or if use of the service was conditional upon giving consent

---

[126] Compare COPPA Rule 16 C.F.R §312.5(a)(2) which expressly provides that parents must be able to consent to the collection and use of personal information without consenting to the disclosure of that information to third parties. Also compare The California Consumer Privacy Act of 2018, Cal. Civ. Code §§ 1798.100 - 1798.199 (CCPA) §1798.120(a) and 1798.115(d) – consumers have the right to opt out of the sale of their personal information to third parties, and the further sale of that information by those third parties.

[127] Article 29 Data Protection Working Party, *Opinion 15/2011 on the Definition of Consent* at 19. Also see Article 29 Data Protection Working Party, *Guidelines on Consent under Regulation 2016/679* at 11.

[128] GDPR art 13(2)(e) requires that when personal information is collected directly from the data subject, the notice must stipulate 'whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data'.

[129] Article 29 Data Protection Working Party, *Guidelines on Consent under Regulation 2016/679* at 10–11.

[130] Ibid at 10–11.

to processing that was 'not necessary for the performance of the contract'.[131] Article 7(4) provides that in assessing whether consent was freely given, 'utmost account' is to be taken of whether use of the service was conditional upon consent being given for processing of personal data that was not 'necessary for the performance of the contract'.[132]

This must be assessed in relation to the 'core service provided', with a genuine choice for additional services and data sharing. For example, if a mobile app for photo-editing requires users to permit the collection of location and states that the information will be used to geo-tag photographs and for behavioural advertising, this consent cannot be regarded as freely given for either purpose. The user should be given the choice to use the app to edit photographs without geolocalisation and should separately be given a choice to opt in to behavioural advertising.[133]

GDPR now also explicitly requires consent to be in an intelligible and easily accessible form. The wording must be in clear and plain language,[134] and the placement of consent must be distinguishable from other matters[135] but not 'unnecessarily disruptive' of the service.[136] This is an interpretational issue that forms part of a broader adoption of plain language principles in law, rather than an amendment of the nature of the consent required. Consent cannot be informed consent if the user does not understand the terms in which it is framed or was misled into overlooking the provision by its placement among other unrelated terms.

---

[131] GDPR rec 43. 'In order to ensure that consent is freely given, consent should not provide a valid legal ground for the processing of personal data in a specific case where there is a clear imbalance between the data subject and the controller, in particular where the controller is a public authority and it is therefore unlikely that consent was freely given in all the circumstances of that specific situation. Consent is presumed not to be freely given if it does not allow separate consent to be given to different personal data processing operations despite it being appropriate in the individual case, or if the performance of a contract, including the provision of a service, is dependent on the consent despite such consent not being necessary for such performance.'

[132] This phrase is to be strictly construed. Article 29 Data Protection Working Party, *Opinion 06/2014 on the Notion of Legitimate Interests of the Data Controller under Article 7 of Directive 95/46/EC* (WP 217, 9 April 2014) at 16–17.

[133] Article 29 Data Protection Working Party, *Guidelines on Consent under Regulation 2016/679* at 6.

[134] GDPR rec 42.

[135] GDPR art 7(2). 'If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of such declaration which constitutes an infringement of this Regulation shall not be binding.'

[136] Ibid rec 32. 'If the data subject's consent is to be given following a request by electronic means, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided.'

(ii) Other Grounds of Lawful Processing

Article 6(1)(b)–(f) of GDPR provides for five other grounds of lawful processing, of which three are relevant to the mobile application developers with whom this dissertation is concerned:

> *'(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;*
>
> *(c) processing is necessary for compliance with a legal obligation to which the controller is subject;*
>
> *...*
>
> *(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.'*

Contractual necessity covers any processing of personal information that is 'necessary in the context of a contract or the intention to enter into a contract'.[137]

Legal grounds must be based in EU or EU member State law, and such laws would set out more detailed conditions upon which processing on these grounds can take place.[138]

The breadth of the 'legitimate interests' ground is limited by two guiding principles. First, is the processing lawful in the context of a relevant and appropriate relationship between the controller and the data subject? Secondly, at the time and in the context of collection, would the data subject reasonably expect that processing might take place for that purpose?[139]

---

[137] Ibid rec 44.
[138] Ibid art 6(2) and rec 45.
[139] Ibid rec 47. Processing contrary to the reasonable expectations of a data subject might be an infringement both the right to respect for private and family life and the right to data protection, enshrined in arts 7 & 8 of the Charter of Fundamental Rights of The European Union (2000/C 364/01). Also see the right to respect for private and family life in the Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights, as amended) (ECHR) ETS 5, 213 UNTS 221 and the right to privacy in s 14 of the Constitution of the Republic of South Africa, 1996. The US constitution does not enshrine a separate right of

The legitimate interests of the controller cover processing that is 'strictly necessary' for security or fraud prevention measures.[140] This would include processing by the controller, network providers and security technology service providers to ensure 'availability, authenticity, integrity and confidentiality of stored or transmitted personal data, and the security of the related services offered by, or accessible via, those networks and systems'.[141] The legitimate interests of the controller may extend to processing for the purposes of direct marketing.[142] Further, legitimate interests may include transmitting personal information of clients for 'internal administrative purposes'[143] within a 'group of undertakings.'[144]

Where consent is obtained for certain purposes, personal information can also be processed for further purposes, either by obtaining fresh consent for the new purpose,[145] or without consent, provided those further purposes are 'compatible' with the original purpose,[146] and notice is given to the data subject about the further purposes for which their personal information is processed.[147] The necessary determination requires both the original purpose and the further purpose to be specifically articulated in order to determine how the personal data in question are necessary for both purposes,[148] and further, whether there is a discernible link between the two purposes.[149] In addition, the controller must consider the context in which

---

privacy outside of the protection against unreasonable search and seizure by governments. A right to privacy was introduced into the California Constitution.

[140] GDPR rec 47.

[141] Ibid rec 49.

[142] Ibid rec 47.

[143] Ibid rec 48.

[144] Ibid art 4(19). 'Group of undertakings' is defined as 'a controlling undertaking and its controlled undertakings'. Rec 37 provides further that the controlling undertaking should be able to 'exert a dominant influence over the other undertakings by virtue, for example, of ownership, financial participation or the rules which govern it or the power to have personal data protection rules implemented. An undertaking which controls the processing of personal data in undertakings affiliated to it should be regarded, together with those undertakings, as a group of undertakings'. When some of those undertakings are based outside the EU, binding corporate rules for lawful cross-border data transfer must be in place.

[145] Ibid rec 50 makes it clear that where consent is obtained the 'compatibility' of the processing is not relevant. There is no implicit restriction on the types of processing for which consent can be requested.

[146] Ibid art 6(4).

[147] Ibid art 13(3) & art 14(4). 'Where the controller intends to further process the personal data for a purpose other than that for which the personal data were collected, the controller shall *provide the data subject prior to that further processing with information on that other purpose* and with any relevant further information as referred to in paragraph 2' (own emphasis).

[148] None of the data protection principles can be considered in isolation, so although GDPR art 6(4) does not refer to this factor, art 5(1)(b) applies, and requires that the further purpose must be 'specified, explicit and legitimate' and art 5(1)(c) requires that the data be 'adequate, reasonable and limited to what is necessary in relation to the purposes'.

[149] Ibid art 6(4)(a).

the personal data was collected,[150] the nature of the data,[151] the potential impact upon the data subject,[152] and the range of 'appropriate safeguards' available.[153]

Although these provisions on a superficial analysis appear to go beyond the notice and consent framework broadly applicable under US data protection laws,[154] when the detailed interpretative guidelines in article 6(4) are properly applied, the 'further processing' ground is probably no broader than the kinds of processing for internal operations and product improvement and development that are permitted under COPPA and the CCPA. Moreover, to the extent that the specific restrictions contained in the e-Privacy Directive[155] apply to a mobile app, as discussed below, these additional grounds of processing listed in GDPR may not be relied upon, and consent must be obtained.

(iii) Notice

Notice of data collection is fundamental to the exercise by a data subject of their statutory rights to access and request rectification or deletion of personal data, or to object to processing of that data.[156] GDPR contains detailed stipulations about the timing,[157] form[158] and content[159] of the notice to be given to a data subject. Notice must include the identity and contact details of the controller, as well as its data protection officer and EU representative, if any.[160] In addition to

---

[150] Ibid art 6(4)(b). The relationship between the controller and the data subjects is expressly referred to, and it stands to reason that in certain relationships of power imbalance processing for further purposes without seeking fresh consent may not meet the fairness requirement stipulated in art 5(1)(a).
[151] Ibid art 6(4)(c). Like POPIA part B, GDPR in art 9 singles out 'special' personal data, such as race, for additional protection and GDPR requires explicit consent for processing such data. GDPR art 10 restricts processing of criminal convictions and related to data.
[152] Ibid art 6(4)(d).
[153] Ibid art 6(4)(e) lists encryption and pseudonymisation, but it is clearly not intended to be prescriptive.
[154] GDPR of course has a comprehensive scope covering all data processing, whereas the sectoral approach in the US may permit certain types of processing to fall through the proverbial cracks.
[155] e-Privacy Directive 2002/58/EC.
[156] *Bara and Others* (C-201/14) ECLI:EU:C:2015:638 para 33.
[157] GDPR art 13(1) now provides that notice must be given at the time information is collected from the data subject, and art 14(3) provides that where it is collected from another source, within a reasonable period after collection not exceeding one month, and at the latest, when the information is used to contact and communicate with the data subject.
[158] GDPR art 12(1). Notice can be given in writing by electronic means but must be in a 'concise, transparent, intelligible and easily accessible form, using clear and plain language'. Whether language is clear must be determined by the type of data subject addressed in the notice, and GDPR expressly requires that language directed at children be understandable to a child.
[159] Ibid art 13(1) & (2). Art 14 contains materially similar requirements for notice when the data is not collected from the data subject, unless the data subject already has the information or providing notice would be 'impossible or involve disproportionate effort'.
[160] Ibid art 13(1)(a) & (b) and art 14(1)(a) & (b). cf COPPA Rule 16 C.F.R §312, The Online Privacy Protection Act of 2003, Cal. Bus. & Prof. Code §§ 22575–22579 (2004), and CCPA do not expressly require a data protection

specifying clearly what personal information is collected, how it will be used, who it will be shared with,[161] and what rights the data subject has,[162] the notice must now:

1. state the legal basis for processing, including any legitimate interests relied upon;[163]
2. state how long it will store the personal information;[164]
3. state the source of the information (if it is not collected directly from the data subject);[165]
4. identify any third country where processing will take place and inform the data subject about the existence (or absence) of an adequacy decision in respect of its data protection laws, or 'appropriate and suitable' contractual safeguards pursuant to article 49(1);[166]
5. set out the rights of the data subject;[167]
6. expressly state whether it is mandatory to provide the personal information to use the service;[168] and

officer, and do not set out what information must be provided about the controller's identity and contact information.

[161] GDPR art 13(1)(e) & art 14(1)(e). A controller can comply by specifying the 'categories of recipients' or identifying the actual recipients. The obligation to give notice does not obviate the need to store data concerning transfers to third parties in order to be able to respond to requests for access to records of personal information. *Rijkeboer*, C-553/07, EU:C:2009:293, paragraph 59 and 68.

[162] Ibid art 13(2).

[163] Ibid art 13(1)(c) & (d), and art 14(1)(c) & 14(2)(b).

[164] Ibid art 13(2)(a) & art 14(2)(a). If it is impossible to state an exact period, the data subject must be informed of the criteria that will be applied in determining how long to store personal information.

[165] Ibid art 14(2)(f). This includes the source of publicly available information.

[166] Ibid art 13(1)(f) & 14(1)(f) read with Chapter V apply when data is transferred to a third country or an international organisation.

[167] Ibid art 13(2)(b) & (d), and art 14(2)(c) & (e). Under GDPR a data subject has rights to access, correction, erasure and portability of their personal information. A data subject must also be informed of their right to complain to a supervisory authority. COPPA Rule 16 C.F.R §312 includes a right to access, correct and request deletion of personal information about children, but US law does not generally afford such rights. In California the CCPA is intended to give effect to the right to privacy recognised in the California constitution, and the right of Californian's to access their personal information. A covered business must respond to a verified consumer request to access or delete its personal information pursuant to §§1798.100(d) & 1798.105(c). Under CalOPPA) §22572 a privacy policy must inform consumers if there is a process to request access to and correction of their personal information, but unlike GDPR, it does not make it mandatory for all operators or websites and online services to create such a process.

[168] GDPR art 13(2)(e).

7. if the personal information will be used for 'profiling'[169] or 'automated-decision making'[170] about the data subject, provide a 'meaningful'[171] explanation of the logic employed by the artificial intelligence (AI) system, and the impact such decisions may have on the data subject.[172]

In these respects, it goes beyond the 1995 Directive, and the US laws considered earlier.

GDPR also expressly requires notice to be given before any further processing commences[173] and before any information is transferred to a third party.[174]

(e) Application to the Study

In the context of mobile apps, clicking an icon or a check box to accept a privacy policy satisfies the requirement of an 'affirmative' act, but simply installing and using the app where a link to the privacy policy was available to view in the app store, app website, or in the app settings or

[169] Ibid art 4(4). The term 'profiling' is defined as 'any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements'.

[170] Ibid art 22. Although the term is not defined expressly, it includes but is wider than 'profiling' but is restricted for the purposes of GDPR to decisions which have a legal or significant effect. Art 22(1) provides that, subject to the reservations in art 22(2): 'The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.'

[171] Ibid art 13(2)(f) & art 14(2)(g) read with art 22. GDPR does not address the difficulty of explaining such complexities in language that will be meaningful to the average data subject. Complying with the 'transparency' principle is recognised as particularly difficult, and this difficulty applies equally to mobile app developers who use AI and machine learning. See Council of Europe Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108) *Artificial Intelligence and Data Protection: Challenges and Possible Remedies* (Strasbourg, 25 January 2019(T-PD (2018) 09Rev) at 12–14.

[172] Ibid. In such cases art 13(2)(f) and 14(2)(g) require that the notice must provide 'meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject'.

[173] Ibid art 13(3) and art 14(4).

[174] Ibid rec 61 provides: 'Where personal data can be legitimately disclosed to another recipient, the data subject should be informed when the personal data are first disclosed to the recipient. Where the controller intends to process the personal data for a purpose other than that for which they were collected, the controller should provide the data subject prior to that further processing with information on that other purpose and other necessary information. Where the origin of the personal data cannot be provided to the data subject because various sources have been used, general information should be provided.'

account dashboard, does not.[175] User actions to accept a permission request,[176] for example, to access location, can be valid consent provided they are specific, free and informed choices. Consent is valid only for the specific purpose or purposes for which it was given.[177] If the user of a ride-sharing app is prompted with a runtime permission request the first time they use the app to book a ride, acceptance of the permission would indicate consent to the use of their location for the purposes of identifying the closest driver and calculating the ride fare. It may not be obvious to the user that their location information is also being processed to refine the developer's algorithms in order to improve future versions of the app or develop new services. It may be less obvious still that their location information is being shared with advertising networks or service providers who will use it for other purposes that have no discernible link to the app. The permission is not consent for these purposes.

Therefore, additional steps are required to give notice to the user of these practices before they indicate their consent, and to ensure that the consent is free, specific, informed and unambiguous, efforts should be made to determine that the notice reaches the user. In the context of a mobile app, this can be achieved by using a combination of short 'just-in-time' notices and links to the privacy policy. Thus a permission request should include additional information:

> *'[App] wants to access your location. [App] uses your location to provide its service and to serve interest-based advertising. You can control how [App] uses and shares your location from settings [Link to privacy policy].'*

On first using the app, a user should be prompted to accept the terms on which the app processes information. If the privacy policy contains terms that a user may find unexpected (that is, any collection or use of personal information that is not reasonably associated with that type of app), these terms should be clearly highlighted in the privacy policy (for example, by using bold text or clear headings) and additional short form notice could be provided in the app store description of privacy practices, or in a pop-up dialog box displayed

---

[175] For the purpose of facilitating transparency and user control the privacy policy should be accessible in these places to read before download, and to refer back to later. However additional user actions must be logged to enable an app developer to demonstrate user consent. Steps should be taken to determine if the user is a child, and in such cases, verify if the consent is from a parent.

[176] E.g. tapping or swiping the screen. These actions will vary according to the OS.

[177] GDPR art 6(1)(a) refers to consent for 'one or more *specific* purposes'. Recital 32 provides further that the consent given 'should cover all processing activities carried out for the same purpose or purposes. When the processing has multiple purposes, consent should be given for all of them.'

to the user on first use (alongside a link to the privacy policy), which provides for users to select the purposes to which they consent.

Furthermore, it must be possible to give qualified consent. This would require a data subject to have the choice to install the app without consenting to the collection of all information requested, or without consenting to the sharing of such information with third parties, unless this is clearly necessary for the app to function. A privacy policy statement advising users that 'if you do not agree to these terms then do not download or use the app' means that the user is unable to refuse consent without detriment. The temptation may be for app developers to include a reference to third-party data sharing in a privacy policy but draw no attention to it, and to include such a disclaimer to strengthen their case that the user agreed to all terms. However, apart from the business case to be made for increasing consumer trust by highlighting possibly unexpected uses of information and providing users with choices about how their personal information is processed,[178] such contract terms may be regarded as an unenforceable 'unfair term'.[179] Coercing a user into agreeing to targeted advertising to use an essential service (which may, for example, include a banking app or a public utility's app), or that offers advantages users cannot secure without using the app (such a 'driving app' is used by insurers to monitor 'good driving' and offer premium reductions or cashbacks) would arguably be clear cases where such consent was not freely given. On the other hand, monetising a free mobile app utility or game through targeted advertising (provided clear notice of the sharing practices is given) would probably be unobjectionable.[180] However, in all cases, the prudent course would be to provide separately for voluntary 'opt-in' consent for sharing personal information with third parties such as advertisers. In short, to be GDPR-compliant, apps that process the personal information of children should treat the FTC's requirements as

---

[178] Carlos Flavián and Miguel Guinalíu, 'Consumer Trust, Perceived Security and Privacy Policy' (2006) 106 *Industrial Management & Data Systems* 601–620.

[179] GDPR rec 42 provides: 'In accordance with Council Directive 93/13/EEC1 a declaration of consent pre-formulated by the controller should be provided in an intelligible and easily accessible form, using clear and plain language and it should not contain unfair terms.' Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts OJ L 95, 21.4.1993 provides in art 3(1) that such a contract 'shall be regarded as unfair if, contrary to the requirement of good faith, it causes a significant imbalance in the parties' rights and obligations arising under the contract, to the detriment of the consumer.' In *Aziz v Caixa d'Estalvis de Catalunya, Tarragona i Manresa (Catalunyacaixa)* (C-415/11) ECLI:EU:C:2013:164 at para 69, the CJEU suggested that terms would be unfair on this test if one could not 'reasonably assume that the consumer would have agreed to the term concerned in individual contract negotiations'.

[180] Federal Trade Commission, *Mobile Privacy Disclosures Building Trust Through Transparency* (February 2013) at 21.

best practice guidelines.[181] This would require not using targeted advertising, specific opt-in consent from the parent for that practice, and not incentivising children to provide additional information that is unnecessary for the app's functions.

The sharing of personal information with service providers for internal support functions such as provision of aspects of the service, for example, push notifications and payment gateways, data storage, app performance analytics, debugging, and security,[182] is lawful (even without consent) on the grounds that they are necessary for the performance of the contract,[183] and may possibly also fall under the grounds of being necessary for compliance with a legal obligation to which the controller is subject,[184] or necessary in order to protect the vital interests of the data subject or of another natural person.[185] Where service providers will make use of the personal information for further purposes, or where the personal information is shared with third parties, consent is required unless the processing can be justified under the 'legitimate interests' ground.[186]

(f) Data Minimisation

The OECD Guidelines contain an express 'collection limitation' principle:

> *'Collection Limitation Principle 7*
>
> *There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.'*[187]

The explanatory memorandum to the 1980 OECD Guidelines indicates that debate put forward before the expert committee about the general principle was intended to encompass limits to 'put an end to the indiscriminate collection of personal data',[188] which may

---

[181] Further, as noted in ch 4, any app developer should ensure they comply fully with COPPA where any of their users are children under 13, resident in the US.
[182] Compare COPPA Rule 16 C.F.R §312.2 definition on 'internal support for the website or online service'; and CCPA §1798.105(d).
[183] GDPR art 6(1)(b).
[184] Ibid art 6(1)(c).
[185] Ibid art 6(1)(d).
[186] Ibid art 6(1)(f).
[187] OECD, *The OECD Privacy Framework* (2013) para 8. The principle (in identical wording) was included as para 7 in the 1980 guidelines. OECD, *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980).
[188] OECD, *Explanatory Memorandum to the OECD Privacy Guidelines* (1980) para 51.

include provisions about data quality, particular categories of sensitive data, particular collection activities, and limits associated with the purpose of processing.[189] The view was expressed that this included '*possibly*, that data collection should be restricted to the minimum necessary to fulfil the specified purpose' (own emphasis).[190] Yet the OECD Guidelines both in their original formulation, and as amended in the OECD Privacy Framework (2013), do not expressly articulate any obligation to minimise data collection per se. Instead, the purpose for which the data is collected must be specified, and use of the data is limited to such purposes or further compatible purposes.[191] In a similar fashion, the COE Convention 108 requires that data must be 'adequate, relevant and not excessive in relation to the *purposes* for which they are stored' (own emphasis).[192] It was this provision, rather than any absolute requirement to minimise data collection, that was incorporated in the 1995 Data Protection Directive[193] and which is retained (without any expansion or clarification) in GDPR under the guise of 'data minimisation'.[194]

GDPR requires that all processing be lawful, fair and transparent.[195] Although it does not contain any general restriction on the purposes for which data can be processed, it does require notice to the data subject about all purposes of processing, and consent (or some other basis in law) for processing the information for that purpose. GDPR enumerates additional safeguards for a defined category of special personal information.[196]

Thus GDPR contains what is termed a principle of 'data minimisation' in terms of which personal data must be 'adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed'.[197] This is closely related to the principle of

---

[189] Ibid.
[190] Ibid.
[191] OECD, *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, para 9 ('purpose specification' and para 10 ('use limitation').
[192] COE Convention 108 art 5(c).
[193] Data Protection Directive 95/46/EC art 6(1)(c).
[194] GDPR art 5(1)(c). Gellert at 486, rightly, distinguishes this provision from data minimisation as an obligation to collect the least amount of data possible, but argues that the provision reflects the balancing test required for risk management under the GDPR.
[195] Ibid art 5(1)(a).
[196] GDPR art 9. The OECD does not define categories of 'sensitive' or 'special' personal information, on the basis that this may differ 'according to the traditions and attitudes of each Member country'. See OECD, *Explanatory Memorandum to the OECD Privacy Guidelines* para 51. In 1981 the COE Convention 108 included categories of 'special' personal information in art 6 but has no general 'collection limitation') provision. These categories were included in art 8 of the Data Protection Directive 95/46/ECand have been retained in GDPR.
[197] Ibid art 5(1)(c) provides that personal information shall be 'adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation').' cf CalOPPA does not require a

'purpose limitation', which requires that personal information can be processed only for specified purposes (sometimes referred to as the principle of purpose specification) and for further purposes that are compatible with the specified purpose (sometimes referred to as the further processing limitation).[198] It is further subject to the principle of 'data quality'[199] and a 'storage limitation', which requires that data should not be kept in a personally identifiable form for longer than is necessary.[200] These limits should be understood both quantitatively and qualitatively.[201] They apply throughout processing, and data minimisation may therefore also require consideration of whether anonymised or pseudonymised data can be used.[202]

(g) Accountability

Under GDPR the controller is responsible for ensuring that processing complies with all data protection principles.[203] This general principle is supplemented by articles 24 and 25, which provide for the implementation of 'appropriate technical and organisational measures' to ensure and be able to demonstrate such compliance, and the implementation of data protection by design and by default.

> *'Article 24 Responsibility of the controller*
>
> 1. *Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary.*

---

privacy policy to disclose the purposes of data collection and sharing. COPPA Rule 16 C.F.R §312.5 (a) requires verifiable parental consent for any collection, use or disclosure of personal information and any material change in such practices and CCPA §1798.100(b) requires a business to disclose the purpose for which personal information will be used, and prohibits the collection of further personal information without such notice.

[198] GDPR art 5(1)(b) provides that personal information shall be 'collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; …'.

[199] Ibid art 5(1)(d).

[200] Ibid art 5(1)(e).

[201] European Data Protection Board, *Guidelines 4/2019 on Article 25 Data Protection by Design and by Default* (13 November 2019) at 11–12: 'Controllers must consider both the volume of personal data, as well as the types, categories and level of detail … if certain categories of personal data is unnecessary or if detailed data isn't needed because less granular data is sufficient, then any surplus personal data shall not be collected.'

[202] Ibid at 20.

[203] Ibid art 5(2). This principle originates in the OECD, *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, but was not included in the COE Convention until its amended in 2017 and was not included in Data Protection Directive 95/46/EC.

2. *Where proportionate in relation to processing activities, the measures referred to in paragraph 1 shall include the implementation of appropriate data protection policies by the controller.*

3. *Adherence to approved codes of conduct as referred to in Article 40 or approved certification mechanisms as referred to in Article 42 may be used as an element by which to demonstrate compliance with the obligations of the controller.'*

A 2018 study highlighted that several apps were sharing personal information with Facebook as soon as the app was installed, before user consent was obtained.[204] This followed a large-scale study that demonstrated that 42% of free Android apps shared personal information with Facebook.[205] Since this transfer of personal information is enabled by Facebook's software development kit (SDK), both Facebook and the app developer who builds their app using the SDK would be controllers.

In 2018, the Court of Justice of the European Union (CJEU) held the host of a Facebook fan page jointly responsible as a data controller along with Facebook for processing the data of visitors to the fan page even if they did not have a Facebook account and had not consented to the processing.[206] The court held that 'controller' must be given a broad interpretation.[207] While merely using the Facebook platform will not make a user a 'controller', the creator of a fan page selected the demographic criteria according to which Facebook would process the data of visitors to the page. It thus participated in determining the means and purpose of processing and was a joint controller even through it did not ever receive any information in personally identifiable form.[208] This finding is consistent with earlier views expressed by the Article 29 Working Party on Data Protection that one can be a joint controller even if one is not able to fulfil 'directly' all obligations of a controller and that having access to the personal information is not an essential pre-condition for being held to be a controller.[209]

---

[204] Privacy International, *How Apps on Android Share Data with Facebook (even if you don't have a Facebook account)* (2018). The app shares an Android ID and the name of the app that has been installed upon app as soon as it is opened. The app user has not given consent for this sharing. They may also not be a Facebook user and thus have not agreed to Facebook's terms of service.
[205] Reuben Binns and others, 'Third Party Tracking in the Mobile Ecosystem' in *Proceedings of the 10th ACM Conference on Web Science* (ACM, Amsterdam, Netherlands 27–30 May 2018) at 5.
[206] *Wirtschaftsakademie Schleswig-Holstein* (C-210/16) ECLI:EU:C:2018:388.
[207] Ibid para 28. Also see *Google Spain SL and Google Inc* (C-131/12) ECLI:EU:C:2014:317 para 34.
[208] Ibid at 6.
[209] Article 29 Data Protection Working Party, *Opinion 1/2010 on the concepts of "controller" and "processor"* (WP 169, 16 February 2010) at 22.

This addresses an important concern about the 'accountability gap' discussed in this dissertation:

> *'The bottom line should be ensuring that even in complex data processing environments, where different controllers play a role in processing personal data, compliance with data protection rules and responsibilities for possible breach of these rules are [sic] clearly allocated, in order to avoid that the protection of personal data is reduced or that a "negative conflict of competence" and loopholes arise whereby some obligations or rights stemming from the Directive are not ensured by any of the parties.'*[210]

The EU response that such parties are 'joint' controllers is, however, complicated by the remarks of the CJEU that joint responsibility as joint controllers does not imply 'equal' responsibility.[211] The level of responsibility would be determined in accordance with the individual circumstances of each case, such as the stage of processing and different degrees of processing in which each party participated,[212] and liability assigned 'within the framework if its responsibilities, powers and capabilities' [213] and 'the specific features of the processing'.[214] It has been held, in line with this approach, that accountability as controller does not extend to 'operations that precede or are subsequent in the overall chain of processing for which that person does not determine either the purposes or the means'.[215] Thus the duty to notify a data subject about processing and obtain informed consent does not extend to further purposes of processing by another controller.[216]

---

[210] Ibid at 22.
[211] *Wirtschaftsakademie Schleswig-Holstein* para 28, 43 and 44.
[212] Ibid.
[213] *Google Spain SL and Google Inc* (C-131/12) ECLI:EU:C:2014:317 para 38.
[214] *Google LLC, successor in law to Google Inc. v Commission nationale de l'informatique et des libertés (CNIL) "Google (Territorial scope of de-referencing)"* [GC] (C-507/17) ECLI:EU:C:2019:772 para 45.
[215] *Fashion ID GmbH & Co. KG v Verbraucherzentrale NRW eV* (C-40/17) ECLI:EU:C:2019:629 para 74. The case concerned the operator of a website which embedded the Facebook 'like' button on its webpage. The transmission of personal information from the user's browser to Facebook Ireland would occur automatically when they visited the site, without their knowledge and even if they did not click on the 'like' button. The operator of the website was a joint controller in respect of such collection and transmission (but not in respect of any subsequent processing by Facebook).
[216] Ibid para 99–101. Its duty to obtain informed consent was thus limited to the operations for which it jointly determined the means and purpose of processing. Also see Article 29 Data Protection Working Party, *Opinion 2/2010 on Online Behavioural Advertising* (WP 171, 22 June 2010) which placed the obligation to obtain consent for cookie placement on advertising networks, and imposed a more limited obligation on publishers, to notify website visitors about the use of cookies on the site and the general use of cookies to deliver cross-device targeted advertising based on user profiles.

The broad interpretation given to the term 'controller' appears to extend beyond the provisions of GDPR, at least on a literal interpretation. Article 26(1) provides that '[w]here two or more controllers jointly determine the purposes and means of processing, they shall be joint controllers'. The use of the conjunctive 'and' in article 4(7) and article 26 of GDPR is not analysed in the CJEU judgments. The court's interpretation (which in fact refers to the disjunctive 'either the purposes or the means'[217]) indicates that provided a party takes part in the processing for its own purposes, it will be a controller even if it does not determine the means of processing,[218] or have any access to the data collected.[219] These jurisprudential gymnastics were foreshadowed in 2010 in the opinion of the Article 29 Working Party that since the term 'joint controller' was not originally intended to cater for the current forms of 'pluralistic control', it must be interpreted loosely 'as meaning "together with" or "not alone" in different forms and combinations'.[220]

Article 26 of GDPR now requires an 'arrangement' between joint controllers to address their roles and responsibilities (as between the controllers) transparently.[221] Notwithstanding this arrangement (or the absence or inaccuracy of any arrangement), a data subject can exercise his or her rights 'in respect of and against each of the controllers'.[222]

These findings would arguably apply by analogy to the app developer and the developer of any SDK or third-party library in relation to a mobile app.[223] However, this is not to say that an app developer is jointly and severally liable for any processing by such third parties that goes beyond the purpose for which the app developer is processing information.

---

[217] *Fashion ID GmbH & Co. KG v Verbraucherzentrale NRW eV* (C-40/17) ECLI:EU:C:2019:629 para 74.
[218] *Jehovan todistajat* (C-25/17) ECLI:EU:C:2018:551 para 68.
[219] Ibid para 38. Also see *Wirtschaftsakademie Schleswig-Holstein* para 38.
[220] Article 29 Data Protection Working Party, *Opinion 1/2010 on the concepts of "controller" and "processor"* (WP 169, 16 February 2010) at 18.
[221] GDPR art 26(1).
[222] Ibid art 26(3).
[223] The case law remains skimpy, and no case has specifically considered the app developers responsibility. One key issue will be whether the app developer is responsible for all processing (since the developer oversees the code that permits the app to collect and share information) or only for processing that it carries out or authorises. Apps frequently state in their privacy policy that third parties will process the information in accordance with their own privacy policy and that it is the responsibility of the app user to check the third party's privacy terms and conditions.

There is no obligation on the app developer to ensure that such third parties will implement their responsibilities as data controllers. By contrast, the responsible party has specific duties in relation to the performance of a processor outlined in article 28, as follows:

> *'Article 28 Processor*
>
> 1. *Where processing is to be carried out on behalf of a controller, the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject.* '[224]

This article brings into sharp focus the dichotomy between the treatment of processors and third parties. A controller who collects personal information that it intends to share with third parties, even when there is 'partial' sharing of purposes or means of processing,[225] is not obliged to seek guarantees about the technical and organisational measures implemented by that third party. It may have to do so when the parties are joint controllers (to the extent that they process personal information for joint purposes),[226] but not otherwise.

Thus, despite the increasing complexity of data processing operations and role-players, GDPR has not 'fundamentally' altered the basis of liability[227] from a 'linear' controller-processor relationship[228] which is ill-suited, if not obsolete, in the context of the

---

[224] The article comprises 10 sub-articles which set out in detail the requirements for a written contract and documented instructions between controller and processor. See further European Data Protection Board, *Opinion 14/2019 on the draft Standard Contractual Clauses submitted by the DK SA (Article 28(8) GDPR)* .

[225] Brendan van Alsenoy, 'Liability under EU Data Protection Law: From Directive 95/46 to the General Data Protection Regulation' (2016) 7 (3) *Journal of Intellectual Property, Information Technology & Electronic Commerce Law* 271–288 at 281, asserts that '[i]n the case of "partial joint control" (whereby certain processing operations are performed under the sole control of one controller), responsibility and liability will only be shared with regard to the common (i.e. jointly controlled) processing activities'.

[226] E.g. Article 29 Data Protection Working Party, *Opinion 10/2006 on the Processing of Personal Data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT)* (WP 128, 23 November 2006) at 3. The Art 29 WP reasoned that SWIFT is the data controller with primary responsibility but financial institutions, as a data controller in respect of their client's data, must ensure that SWIFT fully complies with data protection law.

[227] Ibid at 287–288. Van Alsenoy notes that GDPR has introduced some direct liability for processors, but that in the context of multiple controllers, its provisions remain fundamentally unaltered from the Data Protection Directive 95/46/EC, and European tort law.

[228] René Mahieu, Joris van Hoboken and Hadi Asghari, 'Responsibility for Data Protection in a Networked World: On the Question of the Controller, Effective and Complete Protection and Its Application to Data Access Rights in Europe' (2019) 10 (1) *Journal of Intellectual Property, Information Technology and Electronic Commerce Law* 84–104 at 91.

mobile ecosystem,[229] in particular, the use of cloud services and the widespread integration of third party software, online social networks and advertising networks, as described in chapter 2. This is no longer merely a case of multiple controllers, but of multiple, overlapping and indistinct processing operations.[230]

In contrast to the new reality of ubiquitous data processing, GDPR and CJEU case law rests on the assumption that even if there are multiple controllers, discrete processing operations can be identified. Article 82(4) makes joint controllers jointly and severally liable for damage caused by processing which infringes the Regulation.[231] The implementation of this article necessarily requires that the damage can be causally linked to a particular data-processing operation or set of operations under the control of one or more parties. Recent CJEU case law has further restricted the scope of accountability through a 'phase-based' approach to the liability of joint controllers.[232] Scholars have criticised the broad interpretation of the term 'controller' as extending accountability too widely.[233] In fact, the CJEU's approach would present at least two considerable obstacles to enforcing data protection rights in a complex network of relationships such as that present in the mobile apps ecosystem: [234] namely, what stages of processing the app developer participated in, and the degree to which it participated.[235] When seen against the backdrop that the notice and consent requirements do

[229] Omer Tene, 'Privacy Law's Midlife Crisis: Critical Assessment of the Second Wave of Global Privacy Laws.' (2013) 74 (6) *Ohio State Law Journal* 1217–1262 at 1219 and 1253.
[230] Paul de Hert and Vagelis Papakonstantinou, 'The new General Data Protection Regulation: Still a sound system for the protection of individuals?' (2016) 32 *Computer Law & Security Review* 179–194 at 184.
[231] Van Alsenoy at 288. GDPR art 82(4) provides: 'Where more than one controller or processor, or both a controller and a processor, are involved *in the same processing* and where they are, under paragraphs 2 and 3, responsible for any damage caused by processing, each controller or processor shall be held liable for the entire damage in order to ensure effective compensation of the data subject' (own emphasis).
[232] Mahieu and others at 90.
[233] Christopher Millard, 'At this rate, everyone will be a [joint] controller of personal data!' (2019) 9 (4) *International Data Privacy Law* 217–219 at 217. Ivanova at 5 points out that '[w]hile "purposes and means" is consistently used in the case-law as one noun-phrase, influencing somehow the processing (or agreeing to the processing and making it possible) appears to be enough to qualify as determining both the purposes and the means of that processing operation'. Mahieu and others at 93 contrast this approach with earlier German case law which had consistently found that the Facebook fan page administrator controlled neither the processing nor the means (on what the authors term a 'macroscopic' view of the general purpose and means of Facebook, as opposed to a 'microscopic' view of the particular purpose and means by which an administrator sets up the fan page parameters.
[234] On the burden of proof in relation to civil damages, and arguments that it is already unduly onerous, see Van Alsenoy at 274–275.
[235] Mahieu and others at 95. As the authors point out there is no provision in GDPR which deals with 'partial' controllership.

not require disclosure of this information,[236] it is apparent that the approach does not make it any easier for data subjects to enforce their rights,[237] and does little to encourage transparency by large technology providers.[238]

As an alternative, a 'value-chain' approach has been proposed to

> *'delineate the scope of responsibility of a (joint) controller for the whole set of data processing operations starting from the very design phase of the data processing product or service right through the whole data lifecycle with the irreversible deletion of the personal data'.*[239]

While this proposal has as its goal the 'full lifecycle' data protection required by a Privacy by Design approach,[240] it lacks a sound factual and legal foundation. As illustrated in chapter 2, app developers who integrated third party software may not participate in, or even be aware of the further processing carried out by those parties. As such they cannot qualify as 'joint' controllers in respect of that processing.

---

[236] GDPR art 13 and 14, discussed above, and art 15(1)(c) only require a controller to disclose the recipients or category of recipients to whom the personal data has been disclosed. It is therefore up to the data subject to pursue each controller separately to enforce its rights to information about the purposes of processing and categories of personal data concerned. This is a serious blow for transparency and fairness, unless the data subject is informed of the wider context and consequences of processing, as argued by René Mahieu and Joris van Hoboken, 'Fashion-ID: Introducing a Phase oriented Approach to Data Protection?' *European Law Blog* (30 September 2019) <https://europeanlawblog.eu/2019/09/30/fashion-id-introducing-a-phase-oriented-approach-to-data-protection/> accessed 15 August 2020. Also see Jure Globocnik, 'On Joint Controllership for Social Plugins and Other Third-Party Content–a Case Note on the CJEU Decision in Fashion ID' (2019) 50 (8) *IIC-International Review of Intellectual Property and Competition Law* 1033–1044 at 1038, noting that this will now require two consents by two controllers, both before data is collected (in this case before the 'Like' plugin runs).

[237] Jef Ausloos, René Mahieu and Michael Veale, 'Getting Data Subject Rights Right' (2019) 10 (3) *Journal of Intellectual Property, Information Technology and Electronic Commerce Law* 283–309 at 303 argue for an obligation on processors and joint controllers to pass on access requests to all other joint controllers or facilitate a single point of contact.

[238] Millard at 219.

[239] Yordanka Ivanova, 'Data Controller, Processor or a Joint Controller: Towards Reaching GDPR Compliance in the Data and Technology Driven World' (Forthcoming) in Tzanou M (ed), *Personal Data Protection and Legal Developments in the European Union* (IGI Global, 2020), <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3584207> accessed 10 August 2020, at 22.

[240] Ibid at 12 and 16.

III STATUTORY FRAMEWORK FOR e-PRIVACY

(a) e-Commerce Directive

The e-Commerce Directive of 2000[241] sets out mandatory information that must be provided to the recipients of the service about the service provider[242] and its commercial communications.[243] A mobile app is an 'information society service',[244] in that it is offered at a distance, electronically, and at the request of the user of the service, and usually for remuneration.[245] Thus the app developer (or app owner where applicable), as the provider of the service,[246] must supply the information to app users.

The e-Commerce Directive also contains an exemption from civil and criminal liability for third party content, which protects service providers that act as a mere conduit for

---

[241] 'The essential impact of context on organizational behavior' (2006) 31 *Academy of management review* 386–408.

[242] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on Electronic Commerce) OJ L 178/1, 17.7.2000, art 5 requires that information including the name, geographic address, email address, and tax, regulatory and trade registration information must be provided 'easily, directly and permanently … accessible to the recipients of the service'.

[243] Ibid, art 6 requires that every commercial communication, such as a promotional discount or competition, must be clearly identified as such, along with the identity of the person on whose behalf it is offered, and the conditions attached (always subject to Member State law).

[244] Ibid, art 2(a). Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services OJ L 241, 17.9.2015 art 1(1)(b). The term 'service' is defined as 'any Information Society service, that is to say, any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services.' The definition continues:
'For the purposes of this definition:
(i) "at a distance" means that the service is provided without the parties being simultaneously present;
(ii) "by electronic means" means that the service is sent initially and received at its destination by means of electronic equipment for the processing (including digital compression) and storage of data, and entirely transmitted, conveyed and received by wire, by radio, by optical means or by other electromagnetic means;
(iii) "at the individual request of a recipient of services" means that the service is provided through the transmission of data on individual request.'

[245] The fact that a mobile app is free (or offers a free 'basic' version) will not be determinative. See e.g. *Google LLC v Bundesrepublik Deutschland* (C-193/18) ECLI:EU:C:2019:498, para 19, where it was held that although Gmail is free (in its basic version), it is provided for remuneration in the form of advertising or other indirect revenue.

[246] Directive 2000/31/EC on Electronic Commerce, art 2(b). Any natural or legal person providing an information society service is covered by the Directive.

the transmission of content,[247] or who merely cache[248] or host[249] the content.[250] These exemptions apply to intermediaries such as ISPs who facilitate the transfer of data from mobile apps. The exemptions do not apply to the mobile app developer or app owner (who would typically be a data controller under GDPR).

The exemptions may apply to the OS provider, app stores, social network providers and other platforms, to the extent that they do not have knowledge of or control over the contents.[251] To qualify for the exemption, a platform must not modify the information,[252] must not store it beyond what is permitted[253] and must not further process the information (which may bring them within the definition of 'controller' for the purposes of GDPR insofar as they determine the means or purpose of processing).[254] The e-Commerce Directive does not apply any substantive duties in relation to the protection of data or metadata associated with the content, and need not be discussed further.

---

[247] Ibid art 12. This applies to intermediaries such as ISPs, which meet the criteria of art 12 that they do not initiative the transmission, do not select the receiver, do not select or modify the information transmitted.

[248] Ibid art 13. 'Caching' refers to 'automatic, intermediate and temporary storage' of information transmitted in a communication network. To benefit from the exemption, a service provider must comply with the conditions set out in art 13 and meet the key proviso that it acts 'for the *sole purpose* of making more efficient the information's onward transmission to other recipients of the service upon their request' (own emphasis). Caching of app data by mobile app developers thus falls outside the exemption.

[249] Ibid art 14. The E-commerce Directive does not indicate whether 'optimizing' content, such as promoting particular content on the basis of user reviews, downloads, or curated lists of content, continues to qualify for the exemption. The Centre for Democracy and Technology (contrasting the broader US exemption) draws attention to the provision in rec 42 that the exemptions apply insofar as 'the activity is of a mere technical, automatic and passive' nature. Centre for Democracy and Technology, 'Mobile platforms as intermediaries: Liability protections in the United States, the European Union, and Canada' (27 September 2012) <https://cdt.org/wp-content/uploads/pdfs/Mobile-Platforms-As-Intermediaries.pdf> accessed 16 March 2020 at 20.

[250] For discussion of how these requirements are implemented differently in member State national law, with comparative analysis to the law of Canada, see Sonia K Katyal and Leah Chan Grinvald, 'Platform Law and the Brand Enterprise' (2017) 32 *Berkeley Tech LJ* 1135–1182.

[251] See e.g. *Google France SARL and Google Inc v Louis Vuitton Malletier SA and others* [GC] (C-236/08 to C-238/08) ECLI:EU:C:2010:159 in relation to Google's AdWords, and *L'Oréal SA and Others v eBay International AG and Others* [GC] (C-324/09) ECLI:EU:C:2011:474 in relation to the online marketplace, e-Bay.

[252] Directive 2000/31/EC on Electronic Commerce rec 43 provides that 'manipulations of a technical nature which take place in the course of the transmission' remain exempt 'as they do not alter the integrity of the information contained in the transmission'.

[253] Ibid art 12(2) requires that information is not 'stored for any period longer than is reasonably necessary for the transmission', arts 13(1)(e) and 14(1)(b) require a service provider to act 'expeditiously' to remove or disable access to content when required. Art 15 confirms that there is no duty on the service provider to actively monitor content.

[254] See further the analysis of the Centre for Democracy and Technology under the 1995 Data Protection Directive.

(b) The e-Privacy Directive

The e-Privacy Directive of 2002,[255] as amended with effect from May 2011 by Directive 2009/136/EC,[256] provides in article 5(3):

> *'Member States shall ensure that the storing of information, or the gaining of access to information already stored, in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned has given his or her consent, having been provided with clear and comprehensive information, in accordance with Directive 95/46/EC, inter alia, about the purposes of the processing. This shall not prevent any technical storage or access for the sole purpose of carrying out the transmission of a communication over an electronic communications network, or as strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service.'*[257]

Article 5(3) sets a standard that must be complied with by any party that stores or accesses information that is stored on the device of a user in the EU, and which applies to mobile apps.[258]

This means that consent is the only legal basis for the installation of the mobile app on the device, and any processing during usage of the app that relies on reading information from the device or writing information to device storage must also be based on user consent.[259] Consent is subject to the requirements of GDPR in relation to the nature and form of valid

---

[255] e-Privacy Directive 2002/58/EC.

[256] Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) no 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws OJ L 337, 18.12.2009.

[257] Prior to its amendment by art 2(5) of Directive 2009/136/EC the section only provided for notice, and a right to refuse such processing (a right to 'opt out'). It now requires consent for the processing (i.e. 'opt in' consent). The original wording of art 5(3) provided:
'3. Member States shall ensure that the use of electronic communications networks to store information or to gain access to information stored in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned is provided with clear and comprehensive information in accordance with Directive 95/ 46/EC, inter alia about the purposes of the processing, and is offered the right to refuse such processing by the data controller. This shall not prevent any technical storage or access for the sole purpose of carrying out or facilitating the transmission of a communication over an electronic communications network, or as strictly necessary in order to provide an information society service explicitly requested by the subscriber or user.'

[258] Article 29 Data Protection Working Party, *Opinion 02/2013 on apps on smart devices* (WP 202, 27 February 2013) at 7.

[259] Ibid at 16. Also see European Data Protection Board, *Opinion 5/2019 on the Interplay between the ePrivacy Directive and the GDPR, in particular regarding the Competence, Tasks and Powers of Data Protection Authorities* at para 40.

consent.[260] Processing of personal information which is 'sensitive' (special) personal information requires explicit consent, as discussed above. Thus the grounds of contractual necessity, and the legitimate interests of the controller or a third party (discussed above), have a restricted application to non-sensitive personal information that is not read from or written to the device.

As is the case with GDPR, article 5(3) of the e-Privacy Directive applies regardless of where the controller is established, or where the processing takes place, provided the information is accessed on or stored in the device of a user in the EU. However its provisions are slightly wider in three relevant respects. First, the e-Privacy Directive applies directly to any party that accesses or stores information on the device, regardless of whether they are a controller, processor or third party, and regardless of the size or nature of the entity.[261] Secondly, the directive applies to all information, including information that is not 'personal information'.[262] Thirdly, the scope of e-Privacy extends both to natural persons who are the 'user'[263] of the service for personal or business purposes, and to the legitimate interests of legal persons who are subscribers of an electronic communications service.[264] The directive's scope is thus broader than GDPR, which applies only to the personal information of a living, natural, identifiable person. These provisions are not transferable and cannot be waived.[265]

---

[260] Article 29 Data Protection Working Party, *Guidelines on Consent under Regulation 2016/679* at 4, clarifying that the provisions of GDPR regarding consent are not 'additional obligations' excluded from application to e-privacy by art 95 of GDPR. The e-Privacy Directive 2002/58/EC art 2(f) defines consent by reference to Data Protection Directive 95/46/EC. In accordance with article 94(2) of the GDPR, all references to Directive 95/46/EC in the e-Privacy Directive have been replaced with '[Regulation (EU) 2016/679]'.

[261] Article 29 Data Protection Working Party, *Opinion 02/2013 on apps on smart devices* at 7.

[262] Ibid.

[263] e-Privacy Directive 2002/58/EC art 2(a.) The term 'user' is defined as 'any natural person using a publicly available electronic communications service, for private or business purposes, without necessarily having subscribed to this service'. The term 'user' should also be distinguished from the term 'consumer', which applies only when the service is used for non-business purposes. Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive) OJ L 108, 24.4.2002 art 2(i) defines the term 'consumer' as 'any natural person who uses or requests a publicly available electronic communications service for purposes which are outside his or her trade, business or profession'. (The definitions of the Framework Directive 2002/21/EC are expressly incorporated in art 2 of the e-Privacy Directive 2002/58/EC, save as otherwise provided.)

[264] e-Privacy Directive 2002/58/EC art 1(2) read with rec 12. Framework Directive 2002/21/EC art 2(k) defines the term 'subscriber' as 'any natural person or legal entity who or which is party to a contract with the provider of publicly available electronic communications services for the supply of such services'.

[265] Article 29 Data Protection Working Party, *Opinion 02/2013 on apps on smart devices* at 8.

The remaining provisions of the e-Privacy Directive, which protect the content of communications,[266] traffic data[267] and location data,[268] apply only to the providers of publicly available electronic communication services[269] and providers of public communication networks.[270]

Article 5(1) requires Member States to prohibit 'listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic data by persons other than users, without the consent of the users concerned'.

Article 6(1) requires the provider of publicly available communications networks and electronic communication services to erase or anonymise 'traffic data'[271] relating to subscribers and users when it is no longer needed for the transmission of the communication. In terms of article 6(2), traffic data can be stored for purposes of billing and payment recovery, but only for the minimum period necessary and with notice to users pursuant to article 6(4) of what data is processed for this purpose.

In terms of article 6(3), traffic data may be collected beyond what is necessary to transmit a communication or for billing purposes only if the service provider obtains prior, informed consent to use such data for marketing its services or offering value-added services. The traffic data may be collected and retained only to the extent necessary for such marketing

---

[266] e-Privacy Directive 2002/58/EC art 2(b) defines 'communication' as 'any information exchanged or conveyed between a finite number of parties by means of a publicly available electronic communications service'.
[267] Ibid art 6.
[268] Ibid art 9.
[269] Ibid art 2(c). The term 'electronic communications service' is defined as 'a service normally provided for remuneration which consists wholly or mainly in the conveyance of signals on electronic communications networks, including telecommunications services and transmission services in networks used for broadcasting, but exclude services providing, or exercising editorial control over, content transmitted using electronic communications networks and services; it does not include information society services, as defined in Article 1 of Directive 98/34/EC, which do not consist wholly or mainly in the conveyance of signals on electronic communications networks'.
[270] Ibid art 2(d). The term 'public communications network' is defined as 'an electronic communications network used wholly or mainly for the provision of electronic communications services available to the public which support the transfer of information between network termination points'.
[271] Ibid art 2(b). The term 'traffic data' is defined as 'any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof'. Recital 15 indicates that this 'may, inter alia, consist of data referring to the routing, duration, time or volume of a communication, to the protocol used, to the location of the terminal equipment of the sender or recipient, to the network on which the communication originates or terminates, to the beginning, end or duration of a connection. They may also consist of the format in which the communication is conveyed by the network'.

or value-added service, and the user or subscriber can withdraw their consent (to future processing) at any time.

Article 9(1) provides that the 'location data'[272] of subscribers of public communications networks or publicly available electronic communications services may be processed for a 'value-added service',[273] but only if it is made anonymous or with the prior informed consent of the users or subscribers. Notice must inform subscribers of the type of location data, the purposes and duration of processing and whether data will be transferred to a third party. The location data may be collected and retained only to the extent necessary for such value-added service. The user or subscriber can withdraw their consent (to future processing) at any time.

In addition, even where the user consents to processing of their location data, they 'must continue to have the possibility, using a simple means and free of charge, of temporarily refusing the processing of such data for each connection to the network or for each transmission of a communication'.[274] Further, the processing must take place under the authority of the service provider, or the third party providing the value-added service.[275] As explained in chapter 2, even when a mobile app user refuses permission for location tracking, or temporarily turns off location services in device settings, the app developer or third parties may be tracking the user's location using Wi-Fi or Bluetooth connections. Such mechanisms are thus not in full compliance with article 6(2) unless the app is further prohibited from accessing Wi-Fi and Bluetooth without user permission, *and* the app developer provides clear notice that informs the user what the data will be used for, and when and by whom this data will be used, or a clear link to the third parties' privacy policy which provides this information.

---

[272] Ibid art 2(c). The term 'location data' is defined as 'any data processed in an electronic communications network or by an electronic communications service, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service'. Rec 14 indicates that this may include 'may refer to the latitude, longitude and altitude of the user's terminal equipment, to the direction of travel, to the level of accuracy of the location information [which as explained in chapter 2 are collected from on-device sensors such as the GPS, accelerometer, barometer and compass], to the identification of the network cell in which the terminal equipment is located at a certain point in time and to the time the location information was recorded [as explained in chapter 2 in addition to cell site location data, Wi-Fi and Bluetooth connections can provide location data].

[273] Ibid rec 18. 'Value added services may, for example, consist of advice on least expensive tariff packages, route guidance, traffic information, weather forecasts and tourist information.'

[274] e-Privacy Directive 2002/58/EC art 6(2).

[275] Ibid art 6(3).

Lastly, the e-Privacy Directive sets out a data minimisation principle in recital 30:

> *'Systems for the provision of electronic communications networks and services should be designed to limit the amount of personal data necessary to a strict minimum. Any activities related to the provision of the electronic communications service that go beyond the transmission of a communication and the billing thereof should be based on aggregated, traffic data that cannot be related to subscribers or users. Where such activities cannot be based on aggregated data, they should be considered as value added services for which the consent of the subscriber is required.'*

What is relevant in determining whether a mobile app must comply with these stricter provisions[276] is not whether the app uses the internet for data transfer (as almost all do at least some processing off the device), or who owns the infrastructure that makes this communication possible,[277] but whether the service consists 'wholly or mainly' in the conveyance of signals on an electronic communications network.[278] This has been held to include certain over-the-top (OTT) communication[279] services, such as Skype,[280] but not others, such as web-mail.[281]

---

[276] There are other provisions in the e-Privacy Directive such as restrictions on cookies and direct marketing, and requirements for data breach notification, which are outside the scope of this dissertation.

[277] *UPC DTH Sàrl v Nemzeti Média- és Hírközlési Hatóság Elnökhelyettese* (C-475/12) ECLI:EU:C:2014:285, para 43 held that ownership of the infrastructure is of no relevance. What matters is whether the service provider is 'responsible vis-à-vis the end-users for transmission of the signal which ensures that they are supplied with the service to which they have subscribed'.

[278] e-Privacy Directive 2002/58/EC art 2(a). This includes the internet. The term 'electronic communications network' is defined as 'transmission systems and, where applicable, switching or routing equipment and other resources, including network elements which are not active, which permit the conveyance of signals by wire, radio, optical or other electromagnetic means, including satellite networks, fixed (circuit- and packet-switched, including Internet) and mobile terrestrial networks, electricity cable systems, to the extent that they are used for the purpose of transmitting signals, networks used for radio and television broadcasting, and cable television networks, irrespective of the type of information conveyed;'.

[279] An over-the-top (OTT) communication service 'is available on the internet without the participation of a traditional communications operator'. See *Google LLC v Bundesrepublik Deutschland*, para 11. In other words, an OTT communication service relies on an internet connection to send voice, video and chat messages. It is thus distinguishable from traditional fixed line and mobile network voice-calling and SMS services. The term OTT services is used in a different content to refer to content download and streaming services offered over the internet, such as YouTube, Netflix and Apple TV.

[280] *Skype Communications Sàrl v Institut belge des services postaux et des télécommunications (IBPT)* (C-142/18) ECLI:EU:C:2019:460, concerning a referral from the cour d'appel de Bruxelles (Court of Appeal, Brussels, Belgium)in proceedings instituted under the Belgian Loi du 13 juin 2005 relative aux communications électroniques (Law of 13 June 2005 on electronic communications) (Moniteur belge, 20 June 2005, p. 28070).

[281] *Google LLC v Bundesrepublik Deutschland*, concerning a referral from the Oberverwaltungsgericht für das Land Nordrhein-Westfalen (Higher Administrative Court for the Land of North Rhine-Westphalia, Germany) in

Skype offered a VoIP[282] service called SkypeOut that permitted users to connect from their internet-enabled device to a fixed or mobile number covered by the national numbering plan via the public switched telephone network (PSTN). As Skype was remunerated by users for the service and contracted directly with telecommunications service providers to enable the voice signals to be conveyed from the internet to the PSTN, Skype was held to be an electronic communications service provider.[283]

By contrast, Gmail relies on the transfer of data messages as 'packets' over the internet, but has no control over the routing or the third parties who operate the networks.[284] The CJEU thus overruled the decision of the German administrative court in Cologne, which had held that Google was an electronic communications service provider in that, while it was the providers of internet access who in fact convey the signals that carry the data packets, Google 'appropriated' the conveyance of signals for its own purposes.[285] This finding would have had far-reaching consequences for other services which could be said to be 'primarily'[286] concerned with the conveyance of signals over the internet, such as online banking applications.[287] However, the CJEU found that, while Gmail servers control many aspects that are integral to making such a conveyance happen,[288] Google does not actually convey the

---

proceedings instituted under the German Telekommunikationsgesetz (Law on Telecommunications) of 22 June 2004 (BGBl. 2004 I, p. 1190).

[282] Voice over Internet Protocol.

[283] *Skype Communications Sàrl v Institut belge des services postaux et des télécommunications (IBPT)*, para 33–34. The VoIP service was thus an electronic communications service, for which Skype was responsible, and separate from the internet access, for which each user's ISP would be responsible (para 37).

[284] *Google LLC v Bundesrepublik Deutschland*, para 13 & 24. Google itself operates its own network infrastructure but Gmail is not conveyed exclusively on Google's network. Users create a Gmail account, and are assigned a Gmail address by Gmail. Users access the Gmail interface either through an e-Mail client (a program installed on their desktop or mobile device) or they login to the Gmail website (https://mail.google.com) via a web browser. The email is composed with a recipient email address and message by the user who presses 'send'. This breaks the message down into separate data packets which are transmitted to Gmail's server. Gmail identifies the recipient's server by means of the *Domain Name System* (DNS) and the data packets are routed to the target server where they are stored and made available to the recipient in their email inbox. The transfer of data packets over the internet occurs using standardised email-service protocols, such as the *Transmission Control Protocol — Internet Protocol* (TCP-IP) and the *Simple Mail Transfer Protocol* (SMTP). The packets are routed using a dynamic networking protocol which, in simple terms, means that the 'best available' route is followed by each data packet through the various internet sub-networks available, but these networks are operated by third parties and the route cannot be controlled or predicted by the parties sending and receiving messages.

[285] Ibid, para 18.

[286] Ibid, para 21 referring to the argument of the German supervisory authority.

[287] Ibid, para 21. Although all mobile apps rely on the transfer of data over the internet, the definition of an electronic communications service provider expressly excludes an information society service that does not consist 'mainly or wholly' in the conveyance of signals.

[288] Ibid, para 34. It was common cause that Google conveys signals when it uploads and downloads data packets from the internet related to emails sent and received by Gmail account holders. Further (at para 24) the Gmail

signals by which the data message is transmitted on the open internet, nor do they control the third parties who do so.[289] Thus it is internet service providers who provide and are responsible for the electronic communications service, on which Gmail depends.[290]

The e-Privacy Directive envisages that the technical implementation of its principles will be accomplished by approved industry standards, and article 14(3) provides:

> *'Where required, measures may be adopted to ensure that terminal equipment is constructed in a way that is compatible with the right of users to protect and control the use of their personal data, in accordance with Directive 1999/5/EC and Council Decision 87/95/EEC of 22 December 1986 on standardisation in the field of information technology and communications.'*

As will be discussed later in relation to privacy by design in Europe, this provision could be an important part of an effective privacy by design regulatory framework, but it has not been utilised.

(c) The European Electronic Communication Code

The European Electronic Communication Code (EECC) entered into force on 20 December 2018, and must be enacted through Member State law by 21 December 2020.[291] Under the new

---

servers control the authentication ('login') of Gmail users, the assignment of an Internet Protocol (IP) address to the email addresses, and the email service protocol used to route the message.

[289] Ibid, para 24 and 34–38.

[290] Ibid, para 36, referring to submissions by the European Commission, and citing *UPC DTH Sàrl v Nemzeti Média- és Hírközlési Hatóság Elnökhelyettese*, para 43.

[291] Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing The European Electronic Communications Code (Recast) OJ L 321, 17.12.2018 (EECC). Recital 3 & 4 record that in pursuit of Europe's Digital Single Market Strategy (DSM), and following regulatory review, the directive recasts four earlier directives that formed the framework for regulating electronic communications along with the e-Privacy Directive 2002/58/EC, namely:

- Directive 2002/19/EC of the European Parliament and of the Council of 7 March 2002 on access to, and interconnection of, electronic communications networks and associated facilitie(Access Directive), OJ L 108, 24.4.2002;
- Directive 2002/20/EC of the European Parliament and of the Council of 7 March 2002 on the authorisation of electronic communications networks and services (Authorisation Directive) OJ L 108, 24.4.2002;
- The Framework Directive 2002/21/EC;
- Directive 2002/22/EC of the European Parliament and of the Council of 7 March 2002 on universal service and users' rights relating to electronic communications networks and services (Universal Service Directive) OJ L 108, 24.4.2002; and
- Regulation (EC) No 1211/2009 of the European Parliament and of the Council of 25 November 2009 establishing the Body of European Regulators for Electronic Communications (BEREC) and the Office, OJ L 337, 18.12.2009.

definition of an 'interpersonal communications services',[292] any mobile app that enables user-directed interactive communication via an electronic communications network (such as the internet)[293] will be an 'electronic communications service provider'.[294] The communication must be such that it is directly between a finite group of users who determine the recipients or participants.[295] The new definition now covers VoIP and web-mail services. It would clearly also extend to all OTT communication apps permitting direct user communication (by video, voice or chat),[296] but arguably does not extend to online discussion forums where the participants are neither finite, nor determined by the participants. Where an app delivers both content-based services and a communication service, the application of the EECC will be restricted to the communication service. Member States must provide a general authorisation for interpersonal communication services, which may include a requirement to notify the regulatory authority in that Member State of their services.[297] The provision of such a service can be made subject to conditions related to, inter alia, personal data and privacy protection specific to the electronic communications sector in accordance with the e-Privacy Directive 2002/58/EC.[298]

[292] EECC art 2(5). The term 'interpersonal communications service' is defined as 'a service normally provided for remuneration that enables direct interpersonal and interactive exchange of information via electronic communications networks between a finite number of persons, whereby the persons initiating or participating in the communication determine its recipient(s) and does not include services which enable interpersonal and interactive communication merely as a minor ancillary feature that is intrinsically linked to another service'.

[293] Ibid art 2(1). An 'electronic communications network' is defined in almost identical terms to the existing definition on the e-Privacy Directive 2002/58/EC, save that it includes all mobile networks (not 'mobile terrestrial networks') and expressly applies 'whether or not based on a permanent infrastructure or centralised administration capacity'.

[294] Ibid art 2(4). The definition still excludes content providers, but now expressly includes three sub-categories: interpersonal communication services, the conveyance of signals, and internet access services (as defined in art 2(2) of Regulation (EU) 2015/2120 of the European Parliament and of the Council of 25 November 2015 laying down measures concerning open internet access and amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services and Regulation (EU) No 531/2012 on roaming on public mobile communications networks within the Union, OJ L 310, 26.11.2015).

[295] The definition in EECC art 2(5) refers to '*direct* interpersonal and interactive exchange of information via electronic communications networks *between a finite number of persons*' (own emphasis) and stipulates that 'the persons initiating or participating in the communication determine its recipient(s).'

[296] These can be 'number based' services that rely on a national or international numbering system, such as mobile phone number, or a 'number-independent' service.

[297] EECC art 12.

[298] Ibid annex I.

(d) Technical Standards Directives

The e-Privacy Directive intends to facilitate trade in the internal market and remain technologically neutral.[299] However, it recognises the following in recital 46:

> *'The existence of specific rules for electronic communications services alongside general rules for other components necessary for the provision of such services may not facilitate the protection of personal data and privacy in a technologically neutral way. It may therefore be necessary to adopt measures requiring manufacturers of certain types of equipment used for electronic communications services to construct their product in such a way as to incorporate safeguards to ensure that the personal data and privacy of the user and subscriber are protected.'*

The Directive EU 2015/1535[300] provides for technical standards to be approved in relation to information society services. As yet, no technical standards have been adopted under Directive EU 2015/1535 or its predecessor in relation to the mobile apps ecosystem.[301] The Radio Equipment Directive,[302] and its predecessor, the Directive 1999/5/EC on radio and terminal equipment,[303] also provided for the adoption of technical standards but have not been implemented in relation to mobile devices or radio equipment on such devices.

Finally, article 32 requires all controllers and processors to 'implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk' such as encryption and pseudonymisation, and measures to detect breaches and ensure continuity of service. These provisions are supplemented by article 4 of the e-Privacy Directive

---

[299] e-Privacy Directive 2002/58/EC art 14(1) requires Member States to ensure that 'no mandatory requirements for specific technical features are imposed on terminal or other electronic communication equipment which could impede the placing of equipment on the market and the free circulation of such equipment in and between Member States.' Where such measures are necessary, they are to be adopted through the Commission.

[300] Directive (EU) 2015/1535. This replaces the Directive 98/34/EC of the European Parliament and of the Council of 22 June 1998 laying down a procedure for the provision of information in the field of technical standards and regulations OJ L 204, 21.7.1998 (repealed 6 October 2015).

[301] Directive (EU) 2015/1535 replaces Directive 98/34/EC of the European Parliament and of the Council of 22 June 1998 laying down a procedure for the provision of information in the field of technical standards and regulations OJ L 204, 21.7.1998 (repealed 6 October 2015) but the definition of an information society service remains unchanged.

[302] Directive 2014/53/EU of the European Parliament and of the Council of 16 April 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of radio equipment and repealing Directive 1999/5/EC OJ L 153/62, 22.5.2014 (RE-Directive).

[303] Directive 1999/5/EC of the European Parliament and of the Council of 9 March 1999 on radio equipment and telecommunications terminal equipment and the mutual recognition of their conformity OJ L 91/10, 7.4.1999. Directive 1999/5/EC was repealed by RE-Directive.

and article 40 of the EECC for the providers of public electronic communications services and public communications networks, and the technical standards that have been developed.[304]

(e) The e-Privacy Regulation

The draft e-Privacy Regulation[305] is the focus of regulatory reform efforts aimed at ensuring that electronic communications services provide the same protection of privacy and personal information as traditional communication channels.[306] The European Commission proposal put forward in 2017[307] was amended by proposals advanced in the report of the European Parliament in October 2017.[308] The Regulation remains the subject of protracted negotiations within the Council. The latest draft[309] was rejected by the Permanent Representatives Committee of the Council of the European Union (COREPER) on 22 November 2019, and a new presidential proposal on articles 6 and 8 has been put forward for debate by the Working Party on Telecommunications and Information Society.[310] References are to the latest text of article 6 and article 8 of 21 February 2020, and otherwise to the consolidated text of the Council proposal of 22 November 2019 (with textual indications of amendments of the original Commission proposal). Where comparison is made to key proposals by the European Parliament that are not reflected in this draft, these are indicated by [EP] alongside the text of the proposal.

---

[304] Commission Regulation (EU) no 611/2013 of 24 June 2013 on the measures applicable to the notification of personal data breaches under Directive 2002/58/EC of the European Parliament and of the Council on privacy and electronic communications OJ L 173, 26.6.2013 and European Network and Security Agency, *Technical Guideline on Security measures for Article 4 and Article 13a Version 1.0* (December 2014). Art 40 of the EECC provides for ENISA to continue its role in facilitating the adoption of harmonised technical measures for security across the EU.

[305] Proposal for a regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) Brussels, 10.1.2017 COM(2017) 10 final 2017/0003 (COD).

[306] Ibid rec 6.

[307] Ibid. Although the proposal was introduced in January 2017, several amended proposals have been debated by the Working Party on Telecommunications and Information Society without consensus. The latest Presidential proposal dated 21 February 2020 was discussed on 5 and 12 March 2020: Council of European Union, *Presidential proposal 5979/20* (2017/0003(COD), 21 February 2020).

[308] Proposal for a regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) Brussels, 10.1.2017 COM(2017) 10 final 2017/0003 (COD).

[309] Council of European Union, *Presidential proposal 14054/19* (2017/0003(COD), 15 November 2019). The introduction provides a succinct history of the various compromise texts.

[310] Council of European Union, *Presidential proposal 5979/20*.

The Regulation will apply to publicly available electronic communication services as defined in the EECC,[311] including mobile apps offering OTT services such as instant messaging, web-mail and VoIP, but will also regulate all mobile applications with more stringent provisions relating to access to on-device sensors and information, and storage of information on a user's terminal device.[312] The Regulation is expressly extra-territorial in its application, but requires an electronic communications service provider established outside the EU to appoint a European representative.[313]

The scope of article 5 is wider than article 5(1) of the e-Privacy Directive in that it provides in respect of electronic communications data[314] (which includes both content[315] and metadata[316]):

> *'Article 5 Confidentiality of electronic communications data*
>
> *Electronic communications data shall be confidential. Any interference with electronic communications data, ~~such as by~~ **including** listening, tapping, storing, monitoring, scanning or other kinds of interception, surveillance ~~or~~ **and** processing of electronic communications data, by ~~persons~~ **anyone** other than the end-users **concerned**, shall be prohibited, except when permitted by this Regulation.'*[317]

The provisions for processing by the network or electronic communications service providers are restrictive. Article 6 of the draft Regulation permits processing generally only for the transmission of the communication, the detection of threats to the continuity or security of the

---

[311] Draft e-Privacy Regulation contained in Council of European Union, *Presidential proposal 14054/19* art 4(1)(b).
[312] Ibid art 2(1).
[313] Ibid art 3(2).
[314] Ibid art 4(3)(a). The term 'electronic communications data' is defined as 'electronic communications content and electronic communications metadata'.
[315] Ibid art 4(3)(b). The term 'electronic communications content' is defined as 'the content exchanged by means of electronic communications services, such as text, voice, videos, images, and sound.'
[316] Ibid art 4(3)(c). The term 'electronic communications metadata' is defined as 'data processed ~~in an~~ by means of electronic communications ~~network~~ services for the purposes of transmitting, distributing or exchanging electronic communications content; including data used to trace and identify the source and destination of a communication, data on the location of the device generated in the context of providing electronic communications services and the date, time, duration and the type of communication'. This is thus wider than the definition of traffic data in the e-Privacy Directive.
[317] The prohibition extends beyond art 5(1) of the e-Privacy Directive through the catch-all of any other processing.

service or device, or on legal grounds.[318] Processing is generally permitted only for the duration necessary for the specified purpose(s) and to the extent that the purpose cannot be fulfilled by anonymising the data.[319]

Communications content, which includes text, photos, video and voice data, may be processed only with consent. Sub-point (a), which permits consent to processing necessary for the provision of the service no longer includes the original provisos that processing must be both necessary for and have as its *sole* purpose providing the specific service requested by the end user.[320] It does, however, adopt the European Parliament proposal that consent applies 'purely for individual use',[321] which makes it clear that subpoint (a) would exclude apps integrated with social networking platforms and apps providing electronic communications services. In any event, the processing must not infringe the user's fundamental rights (to privacy and data protection) and the content must be erased when it is no longer necessary for the service.[322] In terms of subpoint (b), processing for all other purposes requires consent from *all* end-users, and a data protection impact assessment is mandatory.[323] Although

---

[318] Council of European Union, *Presidential proposal 14054/19* art 6. The original proposal did not include processing for detection of security risks and under legal obligation, but these inclusions are easily reconciled with art 6 of GDPR.

[319] Council of European Union, *Presidential proposal 5979/20* art 6(2).

[320] Ibid art 6a [prev. 6(3)] provides:

'Permitted processing of electronic communications content

1. Without prejudice to Article ~~(6)~~(1), providers of the electronic communications networks and services ~~may~~ shall be permitted to process electronic communications content only:

~~(a) for the sole purpose of the provision of a specific service to an end-user, if the end-user or end-users concerned have given their consent to the processing of his or her electronic communications content and the provision of that service cannot be fulfilled without the processing of such content; or~~

(a) for the purpose of the provision of an service requested by an end-user for purely individual use if the requesting end-user has given consent and where such requested processing does not adversely affect fundamental rights and interests of another person concerned; or …'.

[321] Draft e-Privacy Regulation proposal for a new article 6(3a).

'The provider of the electronic communications service may process electronic communications data solely for the provision of an explicitly requested service, for purely individual usage, only for the duration necessary for that purpose and without the consent of all users only where such requested processing does not adversely affect the fundamental rights and interests of another user or users.'

[322] Council of European Union, *Presidential proposal 14054/19* art 7(1)

'~~Without prejudice to points (b) of Article 6(1) and points (a), and (b) of Article 6(3)a, t~~The provider of the electronic communications service shall erase electronic communications content or make that data anonymous when it is no longer necessary for the purpose of processing in accordance to article 6(1) and 6a(1) ~~after receipt of electronic communication content by the intended recipient or recipients. Such data may be recorded, or stored by the end-users or by a third party entrusted by them to record, store or otherwise process such data in accordance with Regulation (EU) 2016/679~~.'

[323] Council of European Union, *Presidential proposal 5979/20* art 6a(1)(b) and 6a(2).

anonymisation of the data and notice to supervisory authorities is not mandatory in all cases, [324] it may be indicated by the impact assessment.

The processing of metadata is permitted (in addition to the grounds in article 6(1)) where it is necessary for the service,[325] and is to be erased or anonymised when it is no longer necessary.[326] However, metadata can also be processed where the user has consented to processing.[327] Furthermore, the February 2020 proposal adds an additional basis for processing metadata without consent in pursuit of the legitimate interests of the network or electronic communications service provider,[328] provided that this interest is not overridden by the interests or fundamental rights and freedoms of the end user, particularly a child.[329] Helpfully, the proposal contains two deeming provisions which clarify the limits of the legitimate interests: a user's interests and fundamental rights are deemed to override a service provider's legitimate interests where the metadata contains 'special' personal information, or where the metadata is processed 'to determine the nature and characteristics of the end-user or to build an individual profile of the end-user'.[330] Furthermore, the proposal contains a number of safeguards:

---

[324] In terms of the original draft e-Privacy Regulation art 6(3)(b) consent could only be requested for a purpose that could not be fulfilled by processing anonymous information after consultation of the supervisory authority in terms of art 36 of GDPR.

[325] Council of European Union, *Presidential proposal 5979/20* introduced art 6b(1)(ca): '(ca) it is necessary for the provision of an electronic communications service for which the end-user has concluded a contract.' Art 6b(1)(a) & (b) [prev. art 6(2)(a) & (b)] pertaining to (a) mandatory quality of service requirements, and (b) billing would fall under the new subpoint (ca).

[326] Ibid art 7(2).

[327] draft e-Privacy Regulation art 6(2)(c) applies where 'the end-user concerned has given his or her consent to the processing of his or her communications metadata for one or more specified purposes, including for the provision of specific services to such end-users, provided that the purpose or purposes concerned could not be fulfilled by processing information that is made anonymous.' The Draft e-Privacy Regulation proposal does not impose the requirement to anonymise data wherever possible, but provides that where processing of metadata poses a high risk to fundamental rights such as the rights to privacy and data protection, it must be included in the data protection impact assessment and consultation with supervisory authorities required by articles 35 and 36 of GDPR.

[328] Council of European Union, *Presidential proposal 5979/20* art 6(b) [prev art 6(2)] reads:
'it is necessary for the purpose of the legitimate interests pursued by the electronic communications service or network provider, except when such interest is overridden by the interests or fundamental rights and freedoms of the end-user, in particular where the end-user is a child. The end-user's interests shall be deemed to override the interests of the electronic communications service or network provider if the provider uses the electronic communications metadata to determine the nature and characteristics of the end-user or to build an individual profile of the end-user. The end-user's interests shall also be deemed to override the interests of the provider if the electronic communications metadata contains special categories of personal data referred to in Article 9(1) of Regulation (EU) 2016/679, unless the conditions set out in Article 9(2)(g) and (j) of Regulation (EU) 2016/679 are met'.

[329] The provision thus incorporates the same safeguard as GDPR art 6(1)(f). However, insofar as it permits processing of traffic data, or data read from a device, on a basis other than consent it in fact relaxes the current provisions of the e-Privacy Directive.

[330] Council of European Union, *Presidential proposal 5979/20* art 6(b) [prev art 6(2)].

mandatory anonymisation of the data before it is shared with third parties,[331] a data-protection impact assessment,[332] provision of a clear, easy-to-use and effective opt-out mechanism by which users can object to the processing,[333] and appropriate security measures.[334]

Notably, the Council proposal permits third party processing of electronic communication data.[335] The proposal appears to be an attempt to shoe-horn the activities of third parties (such as ad networks) into the consent framework by requiring compliance with the conditions for processors in article 28 of GDPR. However, this requires not only a contract between the 'processor' and 'controller', but also that the processor 'processes the personal data only on documented instructions from the controller, including with regard to transfers of personal data to a third country or an international organisation',[336] which may not be feasible in the context of most third-party data sharing by mobile apps. At the same time, the Council has deleted article 10 of the original Commission proposal which would have required service providers to ensure that processing by third parties did not exceed the limits of the user's consent, and contains no provisions requiring device manufactures or OS platform providers to create such mechanisms.

Article 8 will have an impact upon all mobile applications and third parties which rely on communications data from mobile apps. Article 8(1) provides:

> *'The use of processing and storage capabilities of terminal equipment and the collection of information from end-users' terminal equipment, including about its software and hardware, other than by the end-user concerned, shall be prohibited, except on the following grounds: …'*

---

[331] Ibid art 6(b)(2).
[332] Ibid art 6(b)(2)(a), read with art 35 and art 36 of GDPR.
[333] Ibid art 6(b)(2)(b).
[334] Ibid art 6(b)(2)(c). E.g. encryption and pseudonymisation.
[335] Council of European Union, *Presidential proposal 14054/19* art 6(3) provides '[a] third party acting on behalf of a provider of electronic communications network or services may be permitted to process electronic communications data in accordance with Articles 6 to 6bc provided that the conditions laid down in Article 28 of Regulation (EU) 2016/679 are met'.
[336] GDPR art 28(3)(a).

The permitted exceptions include the grounds of being necessary for transmission of a communication,[337] user consent,[338] provision of a service requested by the user,[339] location of a device when the user places an emergency call,[340] and 'audience measuring'.[341]

The term 'audience measuring' is not defined,[342] and although anonymous statistics on the number of app downloads and crash reports would appear to be covered, other app analytics providing aggregated data on audience segments (for example, by location, device type, platform, or demographics) and conversion events (for example, opening an app, making an in-app purchase, clicking on an ad, or completing an activity) should not be covered as the information collected may reveal the nature of a particular user (for example, the amount of time spent using a particular app could indicate a user's interests, habits or personality). This is an important distinction as opt-in consent would have to be obtained for such purposes.[343] For app analytics that are covered by the exception, the latest proposal introduces important safeguards: a data protection impact assessment is mandatory,[344] notice and a clear opt-out mechanism must be provided,[345] and appropriate technical and organisational measures such as pseudonymisation and encryption must be implemented.[346] Although such analytics do not

---

[337] Council of European Union, *Presidential proposal 14054/19* art 8(1)(a) [mirroring the original draft e-Privacy Regulation art 8(1)(a)].
[338] Council of European Union, *Presidential proposal 14054/19* art 8(1)(b) [mirroring the original draft e-Privacy Regulation art 8(1)(b)].
[339] Council of European Union, *Presidential proposal 14054/19* art 8(1)(c) [the original draft e-Privacy Regulation art 8(1)(c) was restricted to an 'information society service'].
[340] Council of European Union, *Presidential proposal 14054/19* art 8(1)(f).
[341] Ibid art 8(1)(g).
[342] The term is not defined. Recital 21a provides that '[c]ookies can also be a legitimate and useful tool, for example, in assessing the effectiveness of a delivered information society service, for example of website design and advertising or by helping to measuring web traffic to the numbers of end-users visiting a website, certain pages of a website *or the number of end-users of an application*. This is not the case, however, regarding cookies and *similar identifiers used to determine the nature of who is using the site, which always require the consent* of the end-user. Information society providers that engage in configuration checking to provide the service in compliance with the end-user's settings and the mere logging of the fact that the end-user's device is unable to receive content requested by the end-user should not constitute access to such a device or use of the device processing capabilities'.
[343] Council of European Union, *Presidential proposal 14054/19* rec 20 provides that '[u]se of the processing and storage capabilities of terminal equipment or to access to information stored in terminal equipment without the consent of the end-user should be limited to situations that involve only very limited, intrusion of privacy.' E.g. session cookies to authenticate a user, or remember information entered into forms or items placed in a shopping cart across several web pages in that session. No examples relevant to mobile apps are given in the recital.
[344] Council of European Union, *Presidential proposal 5979/20* art 8(1a)(a).
[345] Ibid art 8(1a)(b). The notice must 'inform the end-user of the envisaged processing operations based on paragraph 1(g) and of the end-user's right to object to such processing, free of charge, at any time, and in an easy and effective manner.'
[346] Ibid art 8(1a)(c).

need to be performed by the service provider itself,[347] the data must be anonymised before it is transferred to a 'third party',[348] or handled by a processor acting in terms of a contract with, and on the documented instructions of, the service provider(s), pursuant to article 28 of GDPR.[349] If those third parties further process aggregated statistics combined from multiple service providers' users should be notified.[350]

The February 2020 proposal has added a further exception for the legitimate interests of the service provider, provided this interest is not overridden by the interests or fundamental rights and freedoms of the end user.[351] This is deemed to be the case in three instances: where the user is a child,[352] where the information is 'special' personal information, and where the information is collected to determine the nature and characteristics of the end-user or to build an individual profile of the user. Recital 21, added in the February 2020 proposal, makes it clear that the legitimate interests ground is not a broad catch-all provision:

> *'The demonstration of a legitimate interest requires careful assessment, in particular whether an end-user can reasonably expect that the use of processing and storage capabilities of her or his terminal equipment or the collection of information from it, may take place.'*

Thus, as a matter of best practice, and in all cases of doubt, consent should be obtained.

Further, article 8(2) prohibits the collection of connectivity data such as network and Wi-Fi connections save for establishing or maintaining a connection[353] or providing the

---

[347] Cf original draft e-Privacy Regulation art 8(1)(d) which referred to 'web audience measuring … carried out by the provider of the information society service requested by the end-user.'

[348] The latest proposal attempts to clarify the term 'third party' in recital 19 as 'a legal or natural person that does not provide an electronic communications service to the end-user concerned'. In a particular context the provider of an electronic communications service could be a third party in respect of another service it offers.

[349] Council of European Union, *Presidential proposal 5979/20* art 8(1a). 'Service providers using processing and storage capabilities of the end-user's terminal equipment or collecting information from the end-user's terminal equipment pursuant to paragraph 1(g) shall not share the information with any third party other than its processors, acting in accordance with Article 28 of Regulation (EU) 2016/679 *mutatis mutandis*, unless it has been made anonymous.'

[350] Cf The Draft e-Privacy Regulation proposal for a proviso to art 8(1)(d) that would curtail such further processing:
'Where audience measuring takes place on behalf of an information society service provider, the data collected shall be processed only for that provider and shall be kept separate from the data collected in the course of audience measuring on behalf of other providers.'

[351] Council of European Union, *Presidential proposal 5979/20* art 8(1)(g).

[352] This effectively means that a mobile app processing information about a child user must obtain parental consent, which is consistent with US law as set out in the Children's Online Privacy Protection Act of 1998, 15 U.S.C. §§ 6501 - 6506 (2018) (COPPA).

[353] Council of European Union, *Presidential proposal 14054/19* art 8(2)(a).

service requested,[354] or (subject to 'clear and prominent' notice of the purpose and modalities of collection and the party responsible for it[355]) after the end user has given consent,[356] or for statistical counting.[357]

Consent of the purposes of the Regulation means freely given, specific, informed affirmative consent compliant with article 4 of GDPR,[358] which can be expressed through 'user-friendly'[359] means such as privacy controls in app settings.[360] Where consent is given it can be withdrawn by the user at any time.[361] However, the Regulation is silent on whether provision of services (even when free to the user) can be conditional upon consent to additional processing, such as that necessary to generate advertising revenue.[362] In the February 2020 proposal, recital 20 is amended to delete the statement that such practices would 'normally not be considered as depriving the end-user of genuine choice if the end-user is able to choose between services'.

Thus, although the e-Privacy Regulation in general expands the basis on which metadata can be collected,[363] its restrictions are far more wide-ranging in respect of mobile apps than article 5(3) of the e-Privacy Directive, and would generally require opt-in consent from the app user to access any on-device sensors or information, unless the data is necessary

---

[354] Ibid art 8(2)(d).
[355] Ibid art 8(2a). 'For the purpose of paragraph 2 points (b) and (c), a clear and prominent notice ~~is~~ shall be displayed informing of, at least, the modalities of the collection, its purpose, the person responsible for it and the other information required under Article 13 of Regulation (EU) 2016/679 where personal data are collected, as well as any measure the end-user of the terminal equipment can take to stop or minimise the collection.'
Further, art 8(2b) requires the implementation of appropriate technical and organisational security measures.
[356] Ibid art 8(2)(b).
[357] Ibid art 8(2)(c). Rec 25 clarifies that this refers to the use of device connections to count or track physical movements such as the number of people in an area. Art 8(2)(c) permits such collection without consent provided the data 'is limited *in time and space* to the extent necessary for this purpose and the data is made anonymous or erased as soon as it is no longer needed for this purpose'.
[358] Ibid art 4a(1), replacing draft e-Privacy Regulation art 9(1).
[359] Council of European Union, *Presidential proposal 14054/19* rec 20a records that users should not be 'overloaded' with consent requests, and that 'user-friendly' and 'transparent' consent practices must be adopted.
[360] Ibid art 4a(2). Art 4a(2a) further provides '[a]s far as the controller is not able to identify a data subject, the technical protocol showing that consent was given from the terminal equipment shall be sufficient to demonstrate the consent of the end-user according Article 8(1)(b)'.
[361] draft e-Privacy Regulation art 9(3).
[362] Cf Draft e-Privacy Regulation proposal for a new art 8(1a) which read:
'(1a) No user shall be denied access to any information society service or functionality, regardless of whether this service is remunerated or not, on grounds that he or she has not given his or her consent under Article 8(1)(b) to the processing of personal information and/or the use of processing or storage capabilities of his or her terminal equipment that is not necessary for the provision of that service or functionality.'.
[363] The current Council proposal is a departure from the requirement of affirmative (opt-in) consent under GDPR (to the extent that metadata may be 'personal information'), and the existing restriction in the e-Privacy Regulation to processing traffic and location data only for first-party marketing or value-added services with user consent.

for transmitting the communication, delivering the service, or otherwise necessary for a legitimate interest of the service provider.

As to accountability, recital 20 records that surreptitious tracking through cookies, web bugs, spyware, device identifiers and device fingerprinting are a 'serious threat' to the privacy of users. The recital provides further:

> *'The responsibility for obtaining consent for the storage of a cookie or similar identifier lies on the entity that makes use of processing and storage capabilities of terminal equipment or collects information from end-users' terminal equipment, such as an information society service provider or ad network provider. Such entities may request another party to obtain consent on their behalf.'*

Parties such as ad networks, analytics providers and cloud storage providers are bound by the prohibition in article 8 in relation to accessing information stored on the device or obtained through on-device sensors, and are thus liable for infringement of those obligations to an administrative fine of up to Euro 10 million, or in the case of an undertaking, 2% of annual turnover in the preceding financial year, whichever is higher.[364]

IV CONCLUSION

This analysis of EU data protection laws illustrates that it is considerably broader than current provisions of US law. Apps must not only have a complete and clear privacy policy. They must ensure that voluntary, specific, informed and affirmative (opt-in) consent is obtained from app users for accessing any information on the device or writing any information to device storage, and for any processing of personal information (outside of the exceptions permitted by GDPR). Use of an app cannot be made conditional upon consent for further processing, and consent can be withdrawn at any time.

The requirements under US law to implement security safeguards are extended to both controllers and processors by article 32 of GDPR and will be extended further by the ePrivacy Regulation to require measures that prevent third parties from processing information without consent.

---

[364] Council of European Union, *Presidential proposal 14054/19* art 23.

Platforms can be held accountable as controllers where they determine the means and purpose of processing. They have an obligation to implement security safeguards where they act as controllers or processors of personal information or electronic communications content or metadata. However, like the US, EU law does not impose any clear requirement on platforms, such as app stores, to screen the content they host.

CHAPTER 6

SA DATA PROTECTION LAW

I INTRODUCTION

Lamentably, until now South Africa has lacked effective and comprehensive data protection, but the Protection of Personal Information Act, Act 4 of 2013 (POPIA), is intended to address that lacuna and will apply to the processing of all personal information. Although its substantive provisions came into operation with effect from 1 July 2020,[1] there will be a one-year grace period,[2] after which all entities processing personal information must ensure that they comply fully with POPIA.

This chapter will discuss the South African approach to data protection. It will set out how POPIA defines personal information, the responsible party, consent (as the primary basis for lawful processing), and other grounds of lawful processing. It will also specifically consider the issues of data minimisation and accountability. These issues were identified in chapter 3 as being central to the analysis of a PbD approach to data protection.

II SOUTH AFRICA'S APPROACH TO DATA PROTECTION

South Africa has adopted the approach of an omnibus data protection statute rather than relying solely on sector-specific legislation, common law protection and self-regulation. Although South Africa is not a member of the OECD and is not a party to the COE Convention, POPIA shares the twin goals articulated in the OECD Guidelines, the COE Convention and GDPR, namely:

1. protecting the individual data subject's fundamental rights and freedoms, principally a right to privacy in relation to their personal information; and
2. removing impediments to the free flow of information, which is in turn underpinned by the values of a democratic and open society, the promise of economic and social progress advanced by new technologies, and by other rights and interests which

[1] Proc R21 *GG* 43461 of 22 June 2020.
[2] POPIA s 114(1).

potentially compete with privacy, including the right of access to information, and the economic interests of parties who process personal information in the course of their business activities.[3]

In particular, the purpose of the Act set out in the preamble[4] and section 2(b)[5] and section 3(3)(a)[6] places importance on interpreting the statute in harmony with international standards, setting down minimum thresholds for lawful processing. In addition, as POPIA is concerned with the protection of the constitutional right to privacy, insofar as a court is required to consider the extent to which processing infringes upon the right to privacy, the Constitution enjoins that international law must be considered, and foreign law may be considered, when interpreting the right.[7]

The Information Regulator is enjoined to exercise its powers and functions with due regard for all of these factors, but also to consider 'any developing general international guidelines relevant to the better protection of individual privacy',[8] This means that the data protection principles set out in POPIA must be interpreted in a manner that takes due consideration of the COE Convention, OECD Guidelines and GDPR, even though these instruments do not impose binding public international law obligations upon South Africa.

III THE RIGHT TO PRIVACY UNDER SOUTH AFRICAN LAW

The preamble to POPIA records that the right to privacy in section 14 of the SA Constitution, 1996, 'includes a right to protection against the unlawful collection, retention, dissemination and use of personal information'.

It is trite that the right to privacy is not absolute. In section 2, POPIA gives privacy special importance as the purpose of the Act is to give effect to this right (or what may

---

[3] Ibid preamble and s 2. Also see s 44(1)(b) which requires the Information Regulator to pay due regard to 'all human rights and social interests that compete with privacy'.
[4] POPIA's preamble records that the Act is intended, inter alia, to 'regulate, in harmony with international standards, the processing of personal information by public and private bodies in a manner that gives effect to the right to privacy subject to justifiable limitations that are aimed at protecting other rights and important interests'.
[5] POPIA s 2(b) provides that the purpose of the Act is, inter alia, to 'regulate the manner in which personal information may be processed, by establishing conditions, in harmony with international standards, that prescribe the minimum threshold requirements for the lawful processing of personal information.'
[6] Ibid s 3(3) provides: 'This Act must be interpreted in a manner that– (a) gives effect to the purpose of the Act set out in section 2'.
[7] Constitution of the Republic of South Africa, 1996 s 39(1)(b).
[8] POPIA s 44(1)(d).

be broadly termed 'informational privacy'). However, POPIA clearly states that this is subject to justifiable limitations,[9] making it clear that all processing must balance the right to privacy against other rights, including a third party's right of access to information,[10] the right of the responsible party or a third party to freedom of expression,[11] and important interests.[12]

IV THE PROTECTION OF PERSONAL INFORMATION ACT (2013) (POPIA)

(a) Origin and Background

The Protection of Personal Information Act (2013) (POPIA)[13] was enacted after detailed investigation of international and foreign data protection regimes and extensive public consultations by the South African Law Reform Commission.[14]

Although POPIA was enacted before the General Data Protection Regulation (2016) (GDPR),[15] it shares many of the same features. This is unsurprising, as POPIA and GDPR have been modelled upon the same data protection principles and the wording of POPIA's provisions reflects the strong influence of GDPR's predecessor, the 1995 Data Protection Directive.[16]

---

[9] A court considering the delicate balancing act required by the statute, would thus need to refer to the provisions of s 36 of the Constitution, and the jurisprudence developed in relation to that provision. A detailed analysis of the application of s 36 to POPIA is beyond the scope of this dissertation.

[10] POPIA s 2(a)(i). Also see Constitution s 32 and Promotion of Access to Information Act 2 of 2000 (PAIA) (PAIA) as amended by POPIA.

[11] Constitution of the Republic of South Africa, 1996 s 16 and POPIA s 7 relating to processing solely for journalistic, literary or artistic purposes.

[12] POPIA s 2(a)(ii).

[13] Ibid.

[14] South African Law Reform Commission, *Project 124 'Privacy and data protection'* (2009), and their earlier work reported on in South African Law Reform Commission, *Discussion Paper 109 Project 124 'Privacy and data protection'* (October 2005) and South African Law Reform Commission, *Issue Paper 24 Project 124 'Privacy and data protection'* (2003).

[15] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA OJ L 119, 4.5.2016 (EU General Data Protection Regulation, GDPR).

[16] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (Data Protection Directive) OJ 1995 L 281/31, 23.11.1995. As indicated further in chapter 8, discusions about the reform of Directive 95/46/EC were already underway when the SALRC drafted its final report in 2009. A first draft of GDPR (released in January 2012) would also have been on the radar of the drafters of POPIA. Proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) Brussels, 25.1.2012 COM(2012) 11 final 2012/0011 (COD).

(b) Personal Information

POPIA applies to the 'processing'[17] of personal information by any 'public'[18] or 'private body'.[19] The term is broadly defined, as follows:

> *'"personal information" means information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person, including, but not limited to–*
>
> *(a) information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the person;*
>
> *(b) information relating to the education or the medical, financial, criminal or employment history of the person;*
>
> *(c) any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other particular assignment to the person;*
>
> *(d) the biometric information of the person;*

---

[17] POPIA s 1. The term 'processing' is defined as 'any operation or activity or any set of operations, whether or not by automatic means, concerning personal information, including—

(a) the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use;

(b) dissemination by means of transmission, distribution or making available in any other form; or
(c) merging, linking, as well as restriction, degradation, erasure or destruction of information'.
The nomenclature used to describe the different processing activities deviates in minor, immaterial respects from GDPR art 4(2) and the 1995 Directive art 2(b). POPIA refers to both an operation and an activity. Although an information processing 'operation' clearly encompasses the operations of a computer processing information automatically, the laws both also extend to manual processing operations. The term 'activity' is used in the Act to encompass any trade, business or professional activity by private or public bodies, including historical, statistical and research activities. See e.g. s 13(1)(a) which restricts processing to a lawful purpose 'related to a function or activity of the responsible party' and the definition of 'private body', 'public body' and 'responsible party' in s 1. Section 6(1)(a) excludes from the ambit of the Act processing 'in the course of a purely personal or household activity.'

[18] POPIA s 1. Like GDPR, POPIA is an omnibus statute regulating processing by government and the private sector. Processing by the state, and the specific exemptions permitted in the national interest lie outside the scope of this dissertation. The term 'public body' as defined includes national, provincial and local government, and functionaries and institutions exercising constitutional and legislative duties, powers and functions.

[19] Ibid s 1. The term 'private body' is defined as
'(a) a natural person who carries or has carried on any trade, business or profession, but only in such capacity; Protection of Personal Information Act, 2013 Act 4 of 2013;
(b) a partnership which carries or has carried on any trade, business or profession; or
(c) any former or existing juristic person,
but excludes a public body;'.

(e) the personal opinions, views or preferences of the person;

(f) correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence;

(g) the views or opinions of another individual about the person; and

(h) the name of the person if it appears with other personal information relating to the person or if the disclosure of the name itself would reveal information about the person;'.

POPIA, like GDPR and its predecessor, the 1995 Data Protection Directive, uses the term 'relating to an identifiable, living natural person' to indicate that any information that may directly or indirectly identify a person is personal information. As is the case in comparable US and EU law, this includes a person's name, identifying numbers, location information, online identifiers, and factors specific to that person's physical, physiological, genetic, mental, economic, cultural or society 'identity'.

It is clear from the use of the term 'including but not limited to' in the definition that the examples given are not intended to be a closed list. Nevertheless, ejusdem generis, they restrict the wide scope of 'information relating to' a person, and require, consistent with the US and EU approach, that the information must not simply relate in a broad sense to the person; it must in fact reveal that person's identity.

It should be emphasised that when the personal information is collected by automated means,[20] such as when it is transferred electronically from a mobile device to the servers of a mobile app developer or cloud provider, it does not matter what form the information takes: structured, semi-structured and unstructured data that contains or reveals personal information will fall within the definition.[21] Personal information in any form or

[20] POPIA s 3(4) provides that '"automated means", for the purposes of this section, means any equipment capable of operating automatically in response to instructions given for the purpose of processing information'. That would clearly cover the collection of data by mobile apps. An explanation of how the mobile app code facilitates processing of data through the device OS is set out in chapter 2.

[21] It is incorrect to regard POPIA as being restricted to personal information that is contained in a 'filing system.' (cf Nomalanga Mashinini 'The processing of personal information using remotely piloted aircraft systems in South Africa' (2020) 53 (1) *De Jure* 140 – 158 at 149). A 'filing system' as defined in POPIA is limited to 'any structured set of personal information', but s 3(1)(a) makes it clear that it is only when personal information is processed by 'non-automated means' that it must form part of a filing system, or be intended to form part of such a system.

medium will constitute a 'record'[22] when it is in the possession or under the control of the app developer, as responsible party. This would include all information produced by the user or their device and recorded or stored in any computer hardware or software.[23]

In relation to mobile apps, POPIA leaves two crucial issues unclear. First, although it is reasonably clear that the phrase 'online identifier or other particular *assignment to the person*' (own emphasis) would cover a username or handle, it is not clear whether it would extend to a device identifier; much less whether it encompasses persistent identifiers such as IMEI numbers, as well as semi-persistent (resettable) advertising identifiers.

Secondly, the status of metadata collected automatically by apps is unclear. It is submitted that the term 'location information' must be widely interpreted to include all data that can be used to reveal or track a person's location through the location of their device (such as network, Wi-Fi and Bluetooth connection data). However, traffic data, apart from location information, does not appear to be covered,[24] as it does not reveal the *contents* of private or confidential communication.[25] Arguably, the definition of 'personal information' is already braodly framed as 'including, but not limited to' the information types specificed and if traffic data could be shown to identify an individual it would be covered. In any event, arguably it is

---

[22] POPIA s 1 defines 'record' as:
'any recorded information-
(a) regardless of form or medium, including any of the following:
  (i) Writing on any material;
  (ii) information produced, recorded or stored by means of any tape-recorder, computer equipment, whether hardware or software or both, or other device, and any material subsequently derived from information so produced, recorded or stored;
  (iii) label, marking or other writing that identifies or describes any thing of which it forms part, or to which it is attached by any means;
  (iv) book, map, plan, graph or drawing;
  (v) photograph, film, negative, tape or other device in which one or more visual images are embodied so as to be capable, with or without the aid of some other equipment, of being reproduced;
(b) in the possession or under the control of a responsible party;
(c) whether or not it was created by a responsible party; and
(d) regardless of when it came into existence'.

[23] Ibid, ss (b) applies both when the information is in the responsible party's possession and when it is *under its control* (such as when it is transferred to cloud storage). Whether data being transferred over the internet is in the app developer's possession or control is a more difficult question to address.

[24] See chapter 2 for a description of the terms metadata and traffic data, and discussion of the extent to which they 'leak' personal information.

[25] POPIA s 1 defines personal information in ss (f) to include 'correspondence' but is expressly restricted to the *content* (and further restricted to correspondence that is 'implicitly or explicitly of a private or confidential nature').

protected under POPIA as part of the 'record' of personal information,[26] being a form of digital address 'label'[27] for personal information being transmitted over an electronic communications network.

Photographs, video files or audio files where a person's image is visible or the person's voice can be heard would be personal information when it is used for biometrics such as facial recognition and voice identification.[28] If the content reveals personal characteristics such as race, gender and age, or the personal opinions, views or preferences of the person, it would also be personal information.[29]

POPIA contains a general prohibition against the processing of 'special' personal information,[30] without the consent of the data subject.[31] Unlike article 9 of GDPR, there is no provision for 'explicit consent'.[32] The requirement for consent does not apply if the

---

[26] POPIA s 3(1) provides that the Act applies to the personal information in a record. Some level of residual protection may be implied by the fact that to protect the personal information the entire record must be secured, but this does not mean that a person processing only traffic data is directly liable for full compliance with POPIA.

[27] A record includes any 'label, marking or other writing that identifies or describes any thing of which it forms part, or to which it is attached by any means' The Electronic Communications and Transactions Act 25 of 2002 (ECTA) s 12 provides:

'A requirement in law that a document or information must be in writing is met if the document or information is-

(a) in the form of a data message; and

(b) accessible in a manner usable for subsequent reference.'

Metadata is not defined in ECTA. Although it is clearly data, which ECTA defines as 'electronic representations of information in any form' it may be separate from (although embedded in or attached to) the 'data message', which is defined as:

'data generated, sent, received or stored by electronic means and includes-

(a) voice, where the voice is used in an automated transaction; and

(b) a stored record;'

The term 'stored record' is not defined in ECTA. See further Lee Swales, 'An analysis of the regulatory environment governing electronic evidence in South Africa: suggestions for reform' (UCT 2019) at 163.

[28] Ibid para (d) of the definition of 'personal information' read with the definition of 'biometrics' as 'a technique of personal identification that is based on physical, physiological or behavioural characterisation including blood typing, fingerprinting, DNA analysis, retinal scanning and voice recognition.'

[29] Ibid para (a) & (e) of the definition of 'personal information'.

[30] Ibid s 26. 'A responsible party may, subject to section 27, not process personal information concerning—

(a) the religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life or biometric information of a data subject; or

(b) the criminal behaviour of a data subject to the extent that such information relates to—

(i) the alleged commission by a data subject of any offence; or

(ii) any proceedings in respect of any offence allegedly committed by a data subject or the disposal of such proceedings.'

GDPR art 9 and art 10 protect the same types of information.

[31] POPIA s 27(1)(a).

[32] Cf GDPR art 9(2)(a). Use of the word 'explicit' under GDPR requires that the consent is not only 'affirmative consent' (which is generally required for all processing) but that the data subject explicitly consents to the specific types of special information and specific purposes of processing.

data has 'deliberately been made public by the data subject'[33] or another ground of lawful processing exists.[34] However, in all cases, the data subject has the right to be notified that the data is being collected.[35]

The personal information of a child may not generally be processed[36] without the consent of a 'competent person'.[37] A child is any person under 18, which provides protection for teenagers, which is absent under the COPPA Rule.[38] However, unlike the COPPA Rule,[39] processing can take place without consent in certain circumstances,[40] and POPIA contains no provisions for 'verified' parental consent.[41]

POPIA does not exclude public information from the definition of personal information, but where information is included in a 'public record'[42] or has 'deliberately' been made public by the data subject, it can be collected from a source other than the data subject,[43] and may be processed further.[44] There is no definition of when information has been made public, which leaves open the situation where personal information that has been shared by a

---

[33] POPIA s 27(1)(e). Similarly see GDPR art 9(2)(e).
[34] POPIA s 27(1)(b)-(d) and s 28 – s 33 provide a number of alternative grounds of processing besides consent. These grounds broadly overlap with the provisions of GDPR art 9(1)(b)-(j).
[35] POPIA s 5(1)(a) read with s 18.
[36] Ibid s 34.
[37] Ibid s 35(1)(a). A 'competent person' is defined in s 1 as 'any person who is legally competent to consent to any action or decision being taken in respect of any matter concerning a child'.
[38] Children's Online Privacy Protection Rule, 16 C.F.R part 312 (COPPA Rule) provides an age of consent as 13. GDPR provides that member states lower the age of consent from 16, but not to below 13.
[39] COPPA Rule 16 C.F.R §312.
[40] Under GDPR art 6(1)(b)-(f) can be relied upon to process the information of a child without parental consent. E.g. Ibid s 6(1)(f) permits processing on the basis of the legitimate interests of the controller and the third party, save where those interests are overridden by the data subject's fundamental rights. There are substantive differences to those grounds the provisions of POPIA s 35(1)(b)–(e), which provide only for the 'exercise of a right or obligation in law', and not for the wider ground of legitimate interests. However, in terms of s 35(1)(e), the information can be processed where it has been 'deliberately been made public by the child with the consent of a competent person'.
[41] GDPR art 8(2) and COPPA Rule 16 C.F.R §312.5(b).
[42] POPIA s 1. The term 'public record' is defined as 'a record that is accessible in the public domain and which is in the possession of or under the control of a public body [as defined], whether or not it was created by that public body'. Where personal information is conveyed to a public body it may not be transferred by that public body to any other person without a lawful basis grounded in POPIA, PAIA or another statute that does not conflict with POPIA.
[43] Ibid s 12(2)(a). Further see s 35(1)(e) as to children: where the information has been deliberately made public with the consent of a competent person the prohibition on processing the information does not apply.
[44] Ibid s 15(3)(b): 'The further processing of personal information is not incompatible with the purpose of collection if–
…
(b) the information is available in or derived from a public record or has deliberately been made public by the data subject;'.

data subject through a social networking platform, for example, is 'public', and can be further processed by the app developer, platform providers, social networks, ad networks and other data subjects.

POPIA does not apply after information has been de-identified. De-identification means that any personal information (that is, information capable of identifying a data subject) has been deleted and there is no 'reasonably foreseeable' means of manipulating the data or linking it to other data in order to re-identify the data subject.[45] This is the equivalent of anonymisation under GDPR.

(c) Responsible Party

The 'responsible party' is 'a public or private body or any other person which, alone or in conjunction with others, determines the purpose of and means for processing personal information'.[46] There can be more than one responsible party. Use of the phrase 'in conjunction with others' makes it clear that they may be acting jointly,[47] but it is equally possible for multiple responsible parties to process the same personal information from a mobile app for their own separate purposes.[48]

---

[45] Ibid s 1. To 'de-identify' personal information means 'to delete any information that–
(a) identifies the data subject;
(b) can be used or manipulated by a reasonably foreseeable method to identify the data subject; or
(c) can be linked by a reasonably foreseeable method to other information that identifies the data subject.

[46] Ibid s 1. This definition is clearly drawn from art 2(d) of the Data Protection Directive 95/46/EC,which is in all material respects identical in art 4(7) of GDPR.. The term encompasses, but is wider than, the 'operator' under COPPA Rule 16 C.F.R §312.

[47] POPIA does not use the word 'jointly' or address the position of joint responsible parties. Cf GDPR art 26. However the term 'in conjunction with' clearly includes persons acting jointly. What is not addressed is whether liability is always joint. E.g. the South African Law Reform Commission, *Project 124 'Privacy and data protection'* at 379 provides the following example of joint liability:
'In terms of POPIA both credit providers and credit bureaux are defined as "responsible parties" and are consequently jointly responsible for the protection of the personal information of data subjects during various stages of the credit reporting cycle.'-However in the same report at 412 it is indicated that the liablity of data exporter and importers (another example of joint controllers) is joint and several. There is no indication in the report if this conclusion is solely in respect of the model clauses then governing cross border data transfers under the Data Protection Direcive 95/46/EC, or whether it applies more broadly to joint responsible parties under POPIA.

[48] It was argued earlier that under GDPR multiple 'controllers' may be acting jointly or separately but that there may also be partial overlap either as to purpose or means of processing or both.

POPIA does not address the responsibilities of the parties in such situations.[49] It may be interpreted as meaning that they are jointly and severally liable[50] for any processing which is carried out jointly (that is to say, where both the purposes and means of processing are shared),[51] but are individually liable for any processing which is carried out separately for their own purposes, and by their own means. However, where there is partial overlap of either the purposes or means of processing, the position is even less clear. In its ordinary meaning the phrase 'in conjunction with' refers to 'the situation in which events or conditions combine or happen together'.[52] It thus includes, but is somewhat wider than, the adjective 'joint' or 'jointly', which means 'belonging to or shared between two or more people'.[53] In each case it would be a question of fact whether responsible parties acted jointly in this sense.

A responsible party may use one or more 'operators'[54] (which has the same meaning as a 'processor' under GDPR and is not to be confused with an 'operator' under COPPA[55]) to carry out all or part of the processing on its behalf. There must be a contract or mandate between the responsible party and the operator,[56] but POPIA contains none of the

---

[49] POPIA s 99(1) permits a data subject (or the Information Regulator at the request of a data subject) to institute a civil action for damages against a responsible party, but does not address the liability of multiple responsible parties who may have been acting in conjunction with one another. Cf GDPR 82(4), which imposes joint and several liability in that multiple controllers or processors can each be sued for the whole of the damage. See further the discussion in chapter 5.

[50] Joint and several liability, which applies to delictual wrongdoers under the common law, entails that each party is liable for the whole of the damages. By contrast in Roman Dutch law co-obligors are liable only jointly (that is for their share of the debt and not in solidum) absent an express or implied intention to the contrary. See *De Pass v The Colonial Govt (1886)* 4 SC 283 at 390 per De Villiers CJ.

[51] This analysis posits that the civil damages permitted under POPIA s 99(1) are delictual in nature, arising from a breach of the right to privacy and the statutory rights enshrined in POPIA, albeit that the section imposes strict liability. Section 99(1) read with s 73 makes a responsible party strictly liable, regardless of any intention or negligence, for a breach of any condition of lawful processing, any provision of ss 22, 54, 69–72 and any code of conduct issued in terms of s 60. Full analysis of this issue lies outside the scope of this dissertation; but see by analogy the obiter remarks of Nicholls J in *Nationwide Airlines (Pty) Ltd (in Liquidation) v South African Airways (Pty) Ltd* 2016 (6) SA 19 (GJ) at 22. See further the discussion of the difference between statutory and delictual damages in *Children's Resource Centre v Pioneer Food* 2013 (2) SA 213 (SCA) at 242 (per Wallis JA) and Malcom Ratz 'Damages Arising from Contraventions of Competition Act 89 of 1998' (2019) 22 *PER* 26.

[52] 'Cambridge English Dictionary' <https://dictionary.cambridge.org/dictionary/english/> accessed 30 March 2020.

[53] Ibid.

[54] POPIA s 1. The term 'operator' is defined as 'a person who processes personal information for a responsible party in terms of a contract or mandate, without coming under the direct authority of that party'. The term 'for' the responsible party has the same meaning as the term 'on behalf of' the data controller under GDPR art 4(8).

[55] Children's Online Privacy Protection Act of 1998, 15 U.S.C. §§ 6501 - 6506 (2018) (COPPA). In terms of §6501(2) personal information can be collected or maintained by another on behalf of the operator of a website or online service. This would be akin to the sub-contracting relationship between a responsible party/data controller and operator/processor under POPIA and GDPR respectively. However, COPPA does not regulate the terms of this sub-contracting relationship, or the liability of the sub-operator.

[56] POPIA definition of 'operator'.

other prescriptions under GDPR so that a general authorisation (rather than documented instructions) would suffice,[57] and a contract which was partly oral and partly written could be utilised, provided that the security obligations of the operator are reduced to writing.[58]

The responsible party will share personal information it collects with the operator (or the personal information may be collected directly by the operator on its behalf), to be processed on behalf of the responsible party. Although POPIA does not stipulate that the written contract must detail the purposes of processing, impliedly the operator may process the personal information only for those purposes, as section 20(a) states that the processor may *only* act with the knowledge and authorisation of the responsible party.[59] This would then mean that notice to and consent from the data subject have been obtained, or another lawful basis for the processing exists. It would further mean that the responsible party is liable for any processing carried out with its knowledge and authorisation. There is no provision of POPIA that would preclude the appointment of a sub-operator (provided this falls within the terms of the authority conferred on the operator). An operator who appoints a sub-processor, or who transfers the personal information to a third party for further processing, without the knowledge or authority of the responsible party, would act in breach of s20(b) of POPIA, which imposes a duty to treat the personal information as confidential, and not to disclose it to any other party (save as authorised by the responsible party or by law).[60]

POPIA envisages that personal information may be transferred to a third party, in pursuit of the legitimate interests of the responsible party or that third party.[61] The terms recipient and third party are not defined. Although the term could include a third party making

---

[57] Ibid s 20. Cf GDPR art 28(3)(a).

[58] POPIA s 21(1) provides that '[a] responsible party must, in terms of a written contract between the responsible party and the operator, ensure that the operator which processes personal information for the responsible party establishes and maintains the security measures referred to in section 19'. Section 21(2) requires the operator to notify the responsible party 'immediately' there are reasonable grounds to be believe that a data breach has occurred.

[59] Ibid s 20 provides:

'An operator or anyone processing personal information on behalf of a responsible party or an operator, must–
(a) process such information only with the knowledge or authorisation of the responsible party; and
(b) treat personal information which comes to their knowledge as confidential and must not disclose it,
unless required by law or in the course of the performance of their duties.'

[60] Ibid. The phrase 'in the course of the proper performance of their duties' is wide enough to encompass a transfer of personal information to a sub-operator, but the use of the conjunctive 'and' between subsec (a) and (b) requires that in addition the operator must do so with the knowledge and authority of the responsible party. Para (b) would preclude transfer to third parties for further processing (for the third parties' purposes rather than for performing duties owed to the responsible party).

[61] Ibid s 11(1)(f).

a request for access to information under the Promotion of Access to Information Act (2000) (PAIA),[62] it extends more widely to include any party who may receive or process the personal information, but will not do so for or under the authority of the responsible party.[63]

Unlike COPPA and GDPR, POPIA does not appear to have extra-territorial application as it only applies where the responsible party is domiciled in South Africa, or where the means of processing are in South Africa. The fact that the personal information relates to a resident of South Africa, is thus not relevant. This could create an undesirable lacuna in the protection offered to South Africans, as many of the most popular apps are developed by parties domiciled elsewhere e.g. the apps considered earlier namely Facebook, YouTube (including YouTube Kids), Zoom and TikTok. In the context of websites, the mere fact that the website is accessible over the internet in a particular country has been found in some US cases to be insufficient to establish the connection required for jurisdiction.[64] Similarly the fact that the mobile application may be downloadable in a particular country would be insufficient to establish that the responsible party is domiciled in that country.

There is an argument to be made that the mobile device itself constitutes part of the means of processing, and therefore POPIA applies when the device (and its user) are located in South Africa.[65] But this is only where it is determined that the device is not used solely to

---

[62] PAIA, as amended by POPIA. In s 1 of PAIA provides:
''third party', in relation to a request for access to–
(a) a record of a public body, means any person (including, but not limited to, the government of a foreign state, an international organisation or an organ of that government or organisation) other than–
  (i) the requester concerned; and
  (ii) a public body; or
(b) a record of a private body, means any other person (including, but not limited to, a public body) other than a requester,
but, for the purposes of sections 34 and 63, the reference to 'person' in paragraphs (a) and (b) must be construed as a reference to 'natural person';'.

[63] See GDPR art 4(10) which defines the term 'third party' as any person who is not the data subject, controller, processor or processing under 'direct authority' of the controller or processor.

[64] See e.g. the California decision in *McDonough v. Fallon McElligott Inc* 40 U.S.P.Q.2d (BNA) 1826, 1828 (S.D. Cal. 1996) which held that maintaining a website accessible to California residents was insufficient to meet the requirement of 'personal jurisdiction' over a non-resident defendant. But in contrast to 'passive' websites see e.g the finding in *Zippo Manufacturing Co v Zippo Dot Com Inc* 952 F. Supp. 1119 (W.D. Pa. 1997) which asserted personal jurisdiction when a website was designed to facilitate commercial exchanges. A discussion of the principles of jurisdiction in 'cyberspace' is beyond the scope of this thesis.

[65] Arguably this casts the net too wide, as it would mean that POPIA applies to non-residents who happen to be in the Republic.

forward information through the Republic.[66] In the case of both websites and mobile apps transmission of data via an internet network alone is unlikely to be considered sufficient to constitute a means of processing.[67] However the mobile application installed on the device and collects information from the sensors and storage on the device before transferring this to the app developer's servers, as explained in chapter 2. Thus a mobile device is central to the means of processing, and arguably distinguishable from websites and other kinds of software.

A mobile application developer is a responsible party. A South African mobile app developer that is domiciled in South Africa must therefore comply with POPIA in respect of all users (including those who are resident outside South Africa) and all processing (regardless of where the processing takes place).

However, where they process the personal information of persons resident in the US and the EU, they would have to ensure that they comply with applicable foreign laws.[68] In relation to proceedings in South Africa or investigations by the Information Regulator in South Africa, section 3(1) of POPIA provides as follows:

> *'(a) This Act applies, subject to paragraph (b), to the exclusion of any provision of any other legislation that regulates the processing of personal information and that is materially inconsistent with an object, or a specific provision, of this Act.*
>
> *(b) If any other legislation provides for conditions for the lawful processing of personal information that are more extensive than those set out in Chapter 3, the extensive conditions prevail.'*

This introduces a considerable degree of complexity to the legal compliance obligations faced by mobile app developers. Where POPIA sets the more stringent standard it must be observed, as it applies to the exclusion of any law that is 'materially inconsistent'.[69]

---

[66] POPIA s 3(1)(b)(ii) provides that the Act applies where the responsible party is 'not domiciled in the Republic, but makes use of automated or non-automated means in the Republic, unless those means are used only to forward personal information through the Republic.'

[67] In the context of determining jurisdiction in the US (discussed earlier) the availability of software for download in a jurisdiction (absent other facts such as collection of payment in that jurisdiction) have been found insufficient.

[68] GDPR and COPPA are expressly extra-territorial and would be enforced by the supervisory authorities against a foreign app developer.

[69] POPIA s 3(2)(a). It is submitted that 'any law' must include any foreign or domestic law that otherwise applies to the processing concerned.

However, POPIA sets out minimum thresholds only for lawful processing, and where another law provides more extensive protection, those provisions would have to be applied.[70]

(d) Conditions of Lawful Processing

POPIA sets out eight conditions of lawful processing,[71] which articulate a set of data protection principles and data subject rights that are closely modelled upon the provisions of the COE Convention, the OECD Guidelines, and the 1995 Data Protection Directive, which were influential in the drafting of POPIA. As such, they are also closely aligned to GDPR (save as outlined below).

Condition 1 is an 'accountability' provision similar to that now included in GDPR.[72]

> *'Condition 1 Accountability*
>
> *8. Responsible party to ensure conditions for lawful processing*
>
> *The responsible party must ensure that the conditions set out in this Chapter, and all the measures that give effect to such conditions, are complied with at the time of the determination of the purpose and means of the processing and during the processing itself.'*

Condition 2 is a processing limitation which encapsulates the requirements of lawfulness, fairness, and data minimisation set out in article 5 of GDPR.

> *'Condition 2 Processing limitation*
>
> *9. Lawfulness of processing*
>
> *Personal information must be processed–*
>
> *(a) lawfully; and*
>
> *(b) in a reasonable manner that does not infringe the privacy of the data subject.*

---

[70] Ibid s 3(2)(b). It is submitted that 'other legislation' would include domestic statutes and regulations enacting sector-specific laws, as well as consumer protection and cybersecurity laws. A South African court and the Information Regulator would not directly enforce a foreign statute, but could indirectly apply its provisions in harmonising the interpretation of POPIA with international standards, or if the law was applicable in accordance with principles of conflict of laws. Thus if a foreign app developer's terms of service stipulate that use of the app is subject to foreign law, that law would apply save to the extent that it is 'materially inconsistent' with POPIA.

[71] Ibid s 4(1).

[72] GDPR art 5(2): 'The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability').

10. Minimality

Personal information may only be processed if, given the purpose for which it is processed, it is adequate, relevant and not excessive.'[73]

The data minimisation principle which underpins the processing limitation condition is supported by the purpose specification and further processing limitation conditions.

'Condition 3 Purpose specification

13. Collection for specific purpose

(1) Personal information must be collected for a specific, explicitly defined and lawful purpose related to a function or activity of the responsible party.

…

14 Retention and restriction of records

(1) Subject to subsections (2) and (3), records of personal information must not be retained any longer than is necessary for achieving the purpose for which the information was collected or subsequently processed, unless–

(a) retention of the record is required or authorised by law;

(b) the responsible party reasonably requires the record for lawful purposes related to its functions or activities;

(c) retention of the record is required by a contract between the parties thereto; or

(d) the data subject or a competent person where the data subject is a child has consented to the retention of the record.

…

Condition 4 Further processing limitation

---

[73] POPIA. There is no material difference between this provision and the provisions of GDPR art 5(1)(a) & (c).
'5. Principles relating to processing of personal data
1. Personal data shall be:
(a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');
…
(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation'); …'.

15 Further processing to be compatible with purpose of collection

(1) Further processing of personal information must be in accordance or compatible with the purpose for which it was collected in terms of section 13.'[74]

Even where personal information is lawfully collected, it must be accurate in a broad sense, which includes information that contains errors (inaccuracies), but also information that is incomplete, outdated or otherwise misleading:

'Condition 5 Information quality

16 Quality of information

(1) A responsible party must take reasonably practicable steps to ensure that the personal information is complete, accurate, not misleading and updated where necessary.'[75]

The responsible party does not act lawfully unless it is also 'open' (that is, transparent) about its data practices.

'Condition 6 Openness

17 Documentation

A responsible party must maintain the documentation of all processing operations under its responsibility as referred to in section 14 or 51 of the Promotion of Access to Information Act.'

This general principle is underpinned by the specific obligations in relation to notice.

---

[74] POPIA. These provisions are comparable to GDPR art 5(1)(b), in terms of which personal data shall be 'collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes …'. The storage limitation in s 14(1) is comparable to art 5(1)(e) which requires that personal data shall be 'kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; …'. These provisions are further discussed below in relation to data minimisation.

[75] GDPR art 5(1)(d) requires that personal data shall be 'accurate, and where necessary, kept up to date'. The proviso to art 5(1)(d) is that 'every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.' Similarly, POPIA s 24 requires a responsible party to correct, destroy or delete inaccurate information 'as soon as reasonably practicable' upon receipt of a request from the data subject. S 24 applies to any personal information that is 'inaccurate, irrelevant, excessive, out of date, incomplete, misleading or obtained unlawfully.'

18 Notification to data subject when collecting personal information

(1) If personal information is collected, the responsible party must take reasonably practicable steps to ensure that the data subject is aware of [the prescribed contents of the notice].'[76]

Further, a responsible party must ensure that personal information is secure from the moment it is collected until it is deleted. When personal information is transferred to an operator (or sub-operator) it remains under the control of the responsible party by virtue of the contract or mandate between the responsible party and the operator. This may not be the case when it is transferred to a third party, who may act as a 'responsible party' in their own right.

'Condition 7 Security Safeguards

19 Security measures on integrity and confidentiality of personal information

(1) A responsible party must secure the integrity and confidentiality of personal information in its possession or under its control by taking appropriate, reasonable technical and organisational measures to prevent–

(a) loss of, damage to or unauthorised destruction of personal information; and

(b) unlawful access to or processing of personal information.'[77]

Thus POPIA, as is the case with the 1995 Directive and GDPR, requires the responsible party to implement 'appropriate technical and organisational measures'[78] to ensure

---

[76] POPIA. These provisions are discussed further below in relation to notice. Compare GDPR art 5(1)(a) which requires that personal data shall be processed 'in a transparent manner', and the detailed provisions of art 13 & 14.

[77] POPIA. The provision is materially similar to GDPR art 5(1)(f) which requires that personal data shall be 'processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ("integrity and confidentiality")'.

[78] Cf GDPR art 24(1) expressly sets out that 'the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons' should be taken into account in determining appropriate measures. Art 32 adds that the 'state of the art', and 'costs of implementation' should also be considered to ensure an appropriate level of security. POPIA refers to 'appropriate and reasonable' measures. The enquiry into whether a measure was reasonably required in the circumstances is usefully informed by the same factors. Neither Act prescribes technical measures, nor do they require necessarily that the most exhaustive or expensive measures be used. However they do require that the measures be kept continuously up to date. Similarly, see *United States v RockYou Inc* Case No 3:12–cv–01487–SI (ND Cal Mar, 27, 2012), an enforcement action under Children's Online Privacy Protection Act of 1998, 15 U.S.C. §§ 6501 - 6506 (2018) (COPPA). The operator of an online service which represented in its privacy policy that it used 'commercially reasonable' measures to safeguard the confidentiality and integrity of personal information. At the time 'Structured Query Language' (SQL) injection and 'Cross-Site Scripting' (XSS) attacks were well-known and well-publicized threats. RockYou! failed to stay informed and to implement the readily available and inexpensive

the security, confidentiality and integrity of personal information in its possession or under its control (that is, held on its behalf by an operator). Section 19(3) requires the responsible party to pay 'due regard' to industry standards and 'generally accepted information security practices and procedures'.

Lastly, the key data subject rights to request access to, correction of, and deletion of information, and to object to processing, are reflected in condition 8 for data subject participation, read with section 5 on data subject rights, and section 71 on automated decision making. POPIA's provisions are comparable to the provisions set out in the 1995 Data Protection Directive[79] and GDPR,[80] but lack the specificity that was introduced by GDPR reforms.[81]

(e) Consent

The grounds of lawful processing under POPIA, like those set out in article 6 of GDPR, include consent, contractual necessity and the legitimate interests of the responsible party or a third party. Even where processing is justified on a basis other than consent, notice is always required and the data subject has a right to object to the processing.[82] Where consent is relied upon, the

---

solutions that existed to prevent such attacks, such as segmenting its servers and storing passwords in encrypted format.

[79] Data Protection Directive 95/46/ECart 12 and 14.

[80] GDPR chapter III (Rights of the data subject), in particular art 15–22.

[81] Thus, when an access request is made, GDPR art 15 provides for detailed disclosures, such as whether the information was used for automated decision making. POPIA simply requires a responsible party to confirm if it 'holds' personal information and which third parties had access to it (but not how it was otherwise processed). GDPR art 20 contains a 'data portability right' expressly requiring the record to be transferred in machine readable format (giving the data subject control over his or her data) whereas POPIA simply requires the record to be supplied 'in a form that is generally understandable'. Lastly, GDPR introduced an express 'right to be forgotten' in art 17 whereas Directive 1995/46/EU only provided for erasure 'as appropriate'. POPIA s 24(1)(a) is more explicit, the data subject the right to request correction or deletion of the information where it is 'inaccurate, irrelevant, excessive, out of date, incomplete, misleading or obtained unlawfully'. It is a matter for interpretation whether these grounds apply to information lawfully collected after consent for the processing is withdrawn and it is no longer necessary to hold the information.

[82] POPIA s 11(3) & (4). The prescribed form for objecting to processing was promulgated in regulations.
In relation to mobile apps this would affect processing based on legitimate interests where no consent was given. The data subject's objection must be made 'on reasonable grounds relating to his, her or its particular situation' and is subject to any legislation permitting such processing. In effect a balancing of the parties' interests is required, and implied POPIA would not permit processing on the grounds of legitimate interests if those interests are overridden by the data subject's interests or fundamental rights. Cf GDPR art 6(1)(f).

consent must be valid, and the processing must also respect all other data-processing conditions to be lawful.[83]

> *'Consent, justification and objection*
>
> *11. (1) Personal information may only be processed if—*
>
> *(a) the data subject or a competent person where the data subject is a child consents to the processing;*
>
> *(b) processing is necessary to carry out actions for the conclusion or performance of a contract to which the data subject is party;*
>
> *(c) processing complies with an obligation imposed by law on the responsible party;*
>
> *(d) processing protects a legitimate interest of the data subject;*
>
> *(e) processing is necessary for the proper performance of a public law duty by a public body; or*
>
> *(f) processing is necessary for pursuing the legitimate interests of the responsible party or of a third party to whom the information is supplied.'*

POPIA provides that the responsible party bears the burden of proof that there is valid consent (where relied upon),[84] and gives the data subject the right to withdraw consent at any time.[85] POPIA does not expressly require that consent is given before collection. However, this is implied by the requirement that personal information 'may only be processed if … the data subject … consents to the processing'.[86]

Consent is defined in POPIA as 'any voluntary, specific and informed expression of will in terms of which permission is given for the processing of personal

---

[83] Article 29 Data Protection Working Party, *Opinion 15/2011 on the Definition of Consent* (WP187, 13 July 2011) at 6–8. Also see Article 29 Data Protection Working Party, *Opinion 06/2014 on the Notion of Legitimate Interests of the Data Controller under Article 7 of Directive 95/46/EC* (WP 217, 9 April 2014) at 9, 10 & 13–14. Both opinions remain relevant under GDPR, and have been endorsed in Article 29 Data Protection Working Party, *Guidelines on Consent under Regulation 2016/679* (WP 259, 28 November 2017).

[84] POPIA s 11(2)(a).

[85] Ibid s 11(2)(b). The savings provision makes it clear that withdrawal of consent does not affect the lawfulness of processing on any other ground, nor does it affect the lawfulness of processing (based on valid consent) prior to the withdrawal of the consent. The unilateral withdrawal of consent (within a reasonable time) was approved in relation to an invasion of privacy (by the publication of personal facts) in *National Media Ltd and another v Jooste* 1996 (3) SA 262 (A) at 647B-C.

[86] POPIA s 11(1)(a). The wording is not framed in the past tense like GDPR art 6(1)(a).

information'.[87] More than mere lip service is to be paid to the requirement for consent. The action of an app user accepting privacy terms, or granting a permission request, will not alone be sufficient proof that consent was validly given.

The requirement for 'voluntary' consent means loosely that consent must be freely given. On closer analysis, the law of contract requires consent to be given by an individual capable of consenting and who is not acting on a misrepresentation, and not under undue influence, duress or bribery.[88] Currently, the extent to which duress is recognised at common law is that a contract is voidable when consent was 'extracted by an unlawful or unconscionable threat of some considerable harm'[89] and there is no broad notion of 'economic' duress (of the kind an app user may feel when choosing between sharing personal information or forgoing use of an otherwise useful (and possibly free) service.

At common law, the concept of duress that vitiates the voluntariness of consent has a more restrictive meaning than the concept of 'freely given',[90] and the onus of proving that consent was not voluntary is on the party alleging it.[91] This restrictive approach is premised upon the sanctity of contract,[92] and the absence of a general duty to point out unexpected terms before presenting a contract for acceptance.[93] Academic arguments have been advanced for a

---

[87] POPIA s 1. Cf GDPR art 4(11) in which 'consent' is defined as 'any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.'

[88] While recognising that these are discrete concepts, it is not intended to discuss the separate elements of each concept, but rather to focus on the common element of vitiating voluntariness of apparent consent. For a similar approach, see Deeksha Bhana, 'Contractual Autonomy Unpacked: The Internal and External Dimensions of Contractual Autonomy Operating in the Post-Apartheid Constitutional Context' (2015) 31 *SAJHR* 526–552, specifically fn 104. For a comprehensive general discussion of the requirements of consent, and the grounds of rescission see R.H. Christie and G. Bradfield, *Christie's Law of Contract in South Africa* (LexisNexis 2016), A.J. Kerr, *The Principles of the Law of Contract* (Butterworths 2002), D. Hutchison and others, *The Law of Contract in South Africa* (OUP 2018) and L.F. Van Huyssteen, M.F.B. Reinecke and G.F. Lubbe, *Contract: General Principles* (Juta 2016). For the co-existence of a delictual cause of action also see J. De Wet and A.L. Van Wyk, *De Wet en Van Wyk: Die Suid-afrikaanse Kontraktereg en Handelsreg : Volume 1 : Kontraktereg* (Butterworths 1992) at 49. As to consent as a justification for an infringement of privacy see Johann Neethling, *Persoonlikheidsreg* (4 edn, Lexis Nexis 2013) at 240–252; J. Neethling, J.M. Potgieter and P.J. Visser, *Law of delict* (Butterworths 1994) and *Financial Mail (Pty) Ltd v Sage Holdings Ltd and Another* 1993 (2) SA 451 (A) at 462–465 and the case law referred to therein. However note that POPIA s 99 provides a statutory right to seek civil damages for breach of its provisions.

[89] *Medscheme Holdings (Pty) Ltd and another v Bhamjee* 2005 (5) SA 339 (SCA) at para 6.

[90] *Hohne v Super Stone Mining (Pty) Ltd* 2017 (3) SA 45 (SCA) at para 28.

[91] Ibid at para 29.

[92] *SA Sentrale Ko-op Graanmaatskappy Beperk v Shifren en andere* 1964 (4) SA 760 (A) at 767A.

[93] *Afrox Healthcare Bpk v Strydom* 2002 (6) SA 21 (SCA).

constitutional concept of consent as an aspect of personal autonomy,[94] and for the development of contract law through the introduction of a general requirement of good faith.[95] At a general level, such arguments have met judicial resistance.[96] The courts have emphasised that they cannot enforce abstract notions of fairness and equity,[97] absent a specific rule embodying the fairness requirement[98] or a clearly demonstrated conflict with the spirt, purport and object of the bill of rights, requiring the incremental development of the common law.[99]

This state of development of the South African common law of contract can be contrasted to the position in the EU. Coercion, vitiating consent, could include social, financial, psychological or other pressures, and special consideration should be given to unequal power relations such as those present in employment relationships and between health providers and patients.[100] Where consent cannot be refused without detriment, or cannot be withdrawn, this could vitiate the voluntariness of consent. A data subject must be informed if the supply of the information is voluntary or mandatory and of any consequences of failure to provide the

---

[94] Bhana. Also see Deeksha Bhana, 'Constitutionalising contract law: Ideology, judicial method and contractual autonomy' (DPhil Wits 2013).

[95] Andre M Louw, 'Yet Another Call for a Greater Role for Good Faith in the South African Law of Contract: Can We Banish the Law of the Jungle, While Avoiding the Elephant in the Room?' (2013) 16 *Potchefstroom Electronic Law Journal* 43–120.

[96] In *BOE Bank Bpk v Van Zyl* 2002 5 SA 165 (C) at para 182–183 it was remarked that our common law has not developed an overarching ground of improperly obtained consent or absence of good faith. Cf remarks in the minority judgment in *Eerste Nasionale Bank van Suidelike-Afrika Bpk v Saayman NO* 1997 (4) SA 302 (SCA) at 318 per Olivier JA. Later in *Brisley v Drotsky* 2002 (4) SA 1 (SCA) at para 22 the court described good faith as a 'controlling principle' based on community standards of fairness. Also see *Barkhuizen v Napier* 2007 (5) SA 323 (CC) at para 82 and *Everfresh Market Virginia (Pty) Ltd v Shoprite Checkers (Pty) Ltd* 2012 (1) SA 256 (CC) at para 72–73.

[97] *Afrox Healthcare Bpk v Strydom* at 32. Also see FJD Brand, 'The Role of Good Faith, Equity and Fairness in the South African Law of Contract: The Influence of the Common Law and the Constitution' (2009) 126 *SALJ* 71–90 and Dusty-Lee Donnelly, 'Do You Always Get Something Out? The Impact of the Insurance Act 18 of 2017 and Revised Policyholder Protection Rules on Material Misrepresentation and Non-disclosure' (2018) 135 *SALJ* 593–612 at 605–606.

[98] E.g. the Protection, Promotion, Development and Management of Indigenous Knowledge Act 6 of 2019, s 1, provides that '"prior informed consent" means the consent in respect of indigenous knowledge granted by a trustee, which has been obtained-

(a) free from any manipulation, interference or coercion;
(b) after full disclosure of the intent and scope of the activity; and
(c) in a language and process understandable to the community.'

[99] *Mighty Solutions CC t/a Orlando Service Station v Engen Petroleum Ltd and another* 2016 (1) SA 621 (CC) para 39. Also see *Barkhuizen v Napier*; and *Makate v Vodacom (Pty) Ltd* 2016 (4) SA 121 (CC) at para 102;

[100] Article 29 Data Protection Working Party, *Working Document on the Processing of Personal Data relating to Health in Electronic Health Records (EHR)* (WP 131, 15 February 2007). Also see Article 29 Data Protection Working Party, *Opinion 8/2001 on the Processing of Personal Data in the Employment Context* (WP 48, 13 September 2001) and Article 29 Data Protection Working Party, *Opinion 5/2004 on Unsolicited Communications for Marketing Purposes under Article 13 of Directive 2002/58/EC* (WP 90, 27 February 2004).

information.[101] Where consent for additional processing that is not essential to provide the service is 'bundled' as a mandatory condition for using a service, it should be presumed not to have been freely given.[102]

It is submitted that a court interpreting the term 'consent' in POPIA should be guided by the EU approach and be clear where POPIA merits departure from the common law concepts of misrepresentation, undue influence, duress and bribery. First, POPIA places the burden of proving that processing is lawful on the responsible party, and thus the responsible party has the onus of proving that consent was voluntary.[103] Secondly, POPIA exhorts courts to interpret the provision consistently with the constitutional right to privacy, and to pay due regard to international data protection law.[104]

Despite the possibility that our courts may give 'voluntary' consent a restricted interpretation, the requirement for 'specific' consent means that broad, or 'blanket', consent to all purposes of processing would not be valid consent under POPIA, as such consent is not given for a specific, and explicitly defined, purpose. This also implies a requirement that those purposes should be specified clearly and precisely in terms which are intelligible to the data subject.[105] Further, it 'cannot apply to an open-ended set of processing activities' but is bounded by the words actually used, in context, and according to the parties' reasonable expectations.[106] If the purpose of further processing was not included in the terms of the consent, then fresh consent must be obtained, unless the purpose can be said to be 'compatible' with the original purpose. Ambiguous terms in a privacy policy or disclosure notice would be interpreted against the drafter (the responsible party) and in favour of the reader (the data subject).[107] Likewise, a misrepresentation in the privacy policy (even if innocent) would vitiate

---

[101] POPIA s 18(1)(d) & (e).
[102] This was the position adopted in relation to Data Protection Directive 95/46/EC. See Article 29 Data Protection Working Party, *Opinion 15/2011 on the Definition of Consent* at 12. Also see GDPR rec 42 & 43, & art 7(4), and Article 29 Data Protection Working Party, *Guidelines on Consent under Regulation 2016/679*at 5.
[103] POPIA s 8.
[104] Ibid s 3. Yvonne Burns and Ahmore Burger-Smidt *A Commentary on the Protection of Personal Information Act* (LexisNexis 2018) at 54.
[105] Article 29 Data Protection Working Party, *Opinion 15/2011 on the Definition of Consent*.
[106] Ibid.
[107] The contra proferentem rule is long established in our law: *South African Railways and Harbours v Cemafrique (Pty) Ltd* 1978 (3) SA 388 (A) at 403F. As to its application in relation to consent and a privacy invasion see *Financial Mail (Pty) Ltd v Sage Holdings Ltd and Another* at 468F-H where Corbett CJ held that where the meaning was unclear the court could adopt 'an equitable construction on the contract and does not adopt a meaning which gives one party an unfair or unreasonable advantage over the other'. Of course this is not to say that the

consent.[108] In both instances, it cannot be said that consent was given for a specific and explicitly defined purpose. Contractual disclaimers would not preclude consent being destroyed by the existence of either a misrepresentation or a justus error,[109] but the provisions of POPIA go further than ordinary protections of contract law.

The ground of consent rests on an uneasy threshold between the law of contract and the law of delict. Contractual doctrines of caveat subscriptor,[110] and quasi mutual assent[111] are, it is submitted, inapposite. Although the terms of any express or implied contract between the app developer and app user must clearly be consulted,[112] the ground of consent under POPIA neither requires nor rests upon the existence of such a contract. It is better understood in terms of the common law doctrines of volenti non fit inuria[113] and waiver, which have been applied to interpret the requirement of informed consent in other contexts.[114] As is the case with informed consent in the medical context, under POPIA, 'consent must not only be informed but also free and voluntary, clear and unequivocal, comprehensive and revocable'.[115]

Therefore, the requirement in POPIA that consent be 'informed' means that the data subject must know and appreciate the nature and extent of any privacy harm or risk and

---

court will rewrite the contract for the parties. See generally as to interpretation of contracts and statutes *Natal Joint Municipal Pension Fund v Endumeni Municipality* 2012 (4) SA 593 (SCA).

[108] *Spindrifter (Pty) Ltd v Lester Donovan (Pty) Ltd* 1986 (1) SA 303 (A) at 316I-J. This principle was cited with approval in *Brink v Humphries & Jewell (Pty) Ltd* 2005 (2) SA 419 (SCA) at para 2, where the Supreme Court of Appeal held, in reliance on *Keens Group Co (Pty) Ltd v Lötter* 1989 (1) SA 585 (C) that such a misrepresentation can consist solely in the furnishing of a misleading contract document, and can ground rescission or render the contract void ab initio where it resulted in a justus error. However, each case will turn on its own facts, and consideration of all relevant evidence may show that the mistake was not reasonable, but rather based on reckless inattention. Cf *Royal Canin South Africa (Pty) Ltd v Cooper and another* 2008 (6) SA 644 (SE).

[109] *Spenmac (Pty) Ltd v Tatrim CC* 2015 (3) SA 46 (SCA) at para 28, referring with approval to Kerr at 253.

[110] Signer beware: the doctrine underscores that the law will not play nursemaid to contracting parties to remake a bad bargain, nor, in the absence of an actionable misrepresentation, impute a duty on the other party to draw attention to onerous provisions.

[111] Although contractual consent is based upon the subjective intention of the parties, the doctrine regards a contract as valid where a party has acted reasonably upon outward objective indications of consent by the other.

[112] *Santam Insurance Co Ltd v Vorster* 1973 (4) SA 764 (A) at 780H–781A and 770H, discussing the interplay between a bilateral contract, volenti non fit inuria and contributory negligence.

[113] The doctrine that a person cannot complain of a harm or risk which they willingly undertook.

[114] The analysis below focusses the requirement for informed consent under medical law and s 12 of the Constitution of South Africa, as to which see generally Michael Bishop and Stu Woolman 'Freedom and Security of the Person' in Woolman S and Bishop M (eds), *Constitutional Law of South Africa*, vol 3 (2 edn) ch 40.11. However informed consent plays an important role in other contexts. See e.g. the discussion of the requirement of full, free, prior informed consent by the community to the exercise of mining rights in *Baleni and Others v Minister of Mineral Resources and Others* 2019 (2) SA 453 (GP), and the inclusion of a requirement for 'prior informed consent' in the Protection, Promotion, Development and Management of Indigenous Knowledge Act 6 of 2019, and in the definition of 'community protocol' in the Copyright Act 98 of 1978, the Trade Marks Act 194 of 1993 and the Designs Act 195 of 1993.

[115] Bishop and Woolman ch 40.11 at fn 415.

consent to the harm or accept the risk.[116] One element does not imply the others, and all three must be present for consent to be 'informed'.[117] This also requires that the consent is comprehensive – covering all aspects of data collection, processing and sharing.

The requirement for 'specific' consent is thus closely related to the requirement that consent be 'informed'. In the mobile apps context, this would require that the data subject must be informed as to which personal information (or types of personal information) will be collected, all purposes for which it will be used and the identity of any third parties who will have access to the information.[118] Unless the data subject has been notified in understandable terms of such matters, and of the possible consequences for him or her, then the consent will not be valid.[119]

POPIA does not refer to 'explicit' consent being required for the processing of special personal information. Nevertheless, if consent is to be 'informed', this implies that the data subject must be made aware that he or she is renouncing the protection afforded to 'special'

---

[116] *Castell v De Greef* 1994 (4) SA 408 (C) at 425H-I/J held that informed consent requires that:
'*(a)* the consenting party 'must have had knowledge and been aware of the nature and extent of the harm or risk';
(b) the consenting party 'must have appreciated and understood the nature and extent of the harm or risk';
(c) the consenting party 'must have consented to the harm or assumed the risk';
(d) the consent 'must be comprehensive, that is extend to the entire transaction, inclusive of its consequences'.
Informed consent in the context of medical law provides a useful analogy, as it is quasi-contractual, being categorised legally as the defence of *volenti non fit injuria to* what would otherwise be an actionable delict for invasion of the patient's rights to bodily integrity, self-determination (*Castell v De Greef* supra at 409B–C and 425C/D–E) and privacy (*Seetal v Pravitha and Another NO* 1983 (3) SA 827 (D)). In a mobile apps context the justification of consent renders lawful what would otherwise be an invasion of the data subject's constitutional right to privacy and statutory right not to have his or her personal information processed without a lawful basis for doing so. The caution of the Supreme Court of Appeal in *Broude v McIntosh and Others* 1998 (3) SA 60 (SCA) at 68A-E and 69E regarding the requirement of unlawfulness does not apply, as processing personal information without a justification set out in s 11 of POPIA is per se unlawful.

[117] *Waring & Gillow Ltd v Sherborne* 1904 TS 340 at 344 per Innes CJ held in relation to the defence of consent: '(I)t must be clearly shown that the risk was known, that it was realised, and that it was voluntarily undertaken. Knowledge, appreciation, consent - these are the essential elements; but knowledge does not invariably imply appreciation, and both together are not necessarily equivalent to consent.'

[118] While it might be unreasonable to expect a responsible party to comprehensively inform a data subject of what further processing the third party will undertake, it must inform them of material facts such as the identity of the third party (which make it possible for the data subject to exercise its rights against that third party). Further, where the third party is located outside South Africa or has been engaged under a contract with the responsible party, the statutory or contractual protection of the data subject's personal information (or absence of such protections) would need to be conveyed.

[119] *Beukes v Smith* 2020 (4) SA 51 (SCA) para 25. By analogy, any matter which the responsible party (or the data subject on being informed of it) might regard as significant must be disclosed. Remote or negligible risks do not need to be disclosed: *Louwrens v Oldwage* 2006 (2) SA 161 (SCA) para 25.

personal information. Written consent is, however, not required.[120] The concept of notice is examined further below.

In the digital era, the spectre of consent being sought for the collection of personal information for broad, ill-defined purposes cannot be ignored. On the one hand, developers may experience genuine difficulty explicitly defining purposes of processing. On the other hand, there is a temptation to draft widely-framed consent terms to cover as yet unanticipated purposes of processing. These considerations exist within a framework of obvious information asymmetry between app developers and the average consumer in relation to how information is collected, used and disclosed. However, POPIA introduces three checks and balances that strengthen the requirement for consent. The first is that POPIA makes it clear in section 9 that processing must not only comply with the letter of the law but must also be carried out 'in a reasonable manner that does not infringe the privacy of the data subject'. Secondly, processing is always subject to the overriding requirement of the principle of minimality in section 10 of POPIA. Personal information collected must be relevant, adequate and not excessive, given the purpose for which it is processed.[121] Thus, even where consent has been given, processing will not be lawful if the processing does not meet the requirement of minimality. Thirdly, the purpose specification condition in section 13 requires that personal information must be collected for 'a specific, explicitly defined and lawful purpose related to a function or activity of the responsible party'.[122] The use of the singular 'purpose' in section 10 and section 13 is a further indication that consent is required separately for each purpose, and global consent to multiple purposes will not meet the requirement for voluntary, specific and informed consent. The proviso in section 13 that the purpose be 'related to a function or activity of the responsible party' goes further than GDPR article 5(1)(b) and article 7. It is a clear indication that POPIA does not permit a privacy policy to include statements such as: 'We share information with our partners and affiliates. They will process that information in accordance with their own privacy policy.' A privacy statement would need to inform a data subject what function of the responsible party is being served by sharing the personal

---

[120] Article 29 Data Protection Working Party, *Working Document on the Processing of Personal Data relating to Health in Electronic Health Records (EHR)* at 9.

[121] In the EU this has been expressed as a requirement that the collection be 'reasonable and necessary' in relation to the purpose for which consent is sought. Article 29 Data Protection Working Party, *Opinion 15/2011 on the Definition of Consent*. Also see Article 29 Data Protection Working Party, *Opinion 03/2013 on Purpose Limitation* (WP 203, 2 April 2013).

[122] POPIA s 13(1).

information and with whom it is being shared, and is valid only in relation to the purpose specified.

It is trite that in South African law, consent can be express or implied. Consent can be in writing, or oral or tacit. Neither POPIA nor GDPR requires consent to be in writing and neither Act requires consent to be expressly given. Consent can be implied from a data subject's actions, such as clicking on an icon, or ticking a checkbox to indicate agreement with a pre-printed consent statement. Consent can also be implied from a clear action alone, such as swiping or clicking to grant permission to access location, after being told why the information is needed. This would imply consent, provided that, in the particular context, it was voluntary, specific and informed. For example, a privacy policy providing full information should be readily accessible to the user before the permission is requested. Importantly, however, the legislation remains flexible and technologically neutral.[123] Although POPIA does not specify any modality for consent,[124] it does refer in the definition to an 'expression of will'.[125] The ordinary meaning of the word 'expression' is 'the act of saying what you think or showing how you feel, using words or actions.[126] As such, it encompasses words and other actions. It does not include silence or inaction. Furthermore, it is not possible to determine objectively from silence that the purported 'consent' is informed.[127] The data subject is not signifying in any way that they are aware of the personal information being collected and the purpose of the said collection. Thus it is submitted that under POPIA, consent cannot be implied from inaction or silence. This means that the 'default' settings must require some action by the data subject to indicate consent before personal information is collected.[128]

---

[123] On the importance of this see the earlier opinion in Article 29 Data Protection Working Party, *Opinion 15/2011 on the Definition of Consent* at 35.

[124] The only exception is Form 4 of the Regulations relating to the Protection of Personal Information in R 1383 *GG* 42110 of 14 December 2018 which requires written signed consent for the receipt of direct marketing material, in terms of s 69(1)(b) of POPIA (i.e. where the person is not an existing customer, and the marketing does not relate to the responsible party's own similar products and services.

[125] There is no discussion in the report of the South African Law Reform Commission of why it adopted this wording, and it is submitted that nothing should be read into the fact that it differs from the use of the word 'indication' in Directive 95/46/EU art 2(h). As a South African statute POPIA is to be interpreted on its own terms (albeit in harmony with international standards). Such an interpretation requires that the words actually used be given their ordinary meaning, in context.

[126] 'Cambridge English Dictionary' <https://dictionary.cambridge.org/dictionary/english/> accessed 30 March 2020.

[127] *Bundesverband der Verbraucherzentralen und Verbraucherverbände - Verbraucherzentrale Bundesverband e.V. v Planet49 GmbH* [GC] (C-673/17) ECLI:EU:C:2019:801 at para 54–55.

[128] Article 29 Data Protection Working Party, *Opinion 15/2011 on the Definition of Consent* at 36.

Thus it is submitted that on a proper interpretation, 'consent' for the purposes of POPIA must be:

1. given prior to processing (that is, before any information is collected);
2. given affirmatively (that is, by 'opt-in' rather than 'opt-out' mechanisms, where the default setting requires user action before any information is collected);
3. given for clearly specified purposes which have been adequately explained; and
4. given freely (that is, any collection that is not reasonable and necessary for the use of the service is not unfairly made a condition of use of the service).[129]

(f) Other Grounds of Lawful Processing

Section 11(1)(b)–(f) of POPIA provides for five other grounds of lawful processing, of which three are relevant to the mobile application developers with whom this dissertation is concerned:

> *'(b) processing is necessary to carry out actions for the conclusion or performance of a contract to which the data subject is party;*
>
> *(c) processing complies with an obligation imposed by law on the responsible party;*
>
> *...*
>
> *(f) processing is necessary for pursuing the legitimate interests of the responsible party or of a third party to whom the information is supplied.'*

These grounds are in all material respects similar to article 5(1)(a), (b) and (f) of GDPR, discussed earlier. While GDPR expressly makes the legitimate interests subject to the overriding rights and interests of the data subject, it is submitted that POPIA section 2 makes it sufficiently clear that all processing must balance the right to privacy against other rights, including a third party's right of access to information, and important interests.[130] In any event, all law is subject to the Constitution, 1996, and must be interpreted in such a way as to give effect to the rights in the bill of rights.

---

[129] These four criteria are expressed in similar terms in relation to Data Protection Directive 95/46/ECin Article 29 Data Protection Working Party, *Working Document 02/2013 Providing Guidance on Obtaining Consent for Cookies* (WP 208, 2 October 2013) at 3.
[130] POPIA s 2(a)(ii).

While the scope of the term 'legitimate interests' is not defined in POPIA, it is submitted that the guiding principles contained in GDPR ought to be instructive in interpreting this provision, namely, determining what is appropriate in the context of the relationship between the responsible party and the data subject, and what would reasonably be expected by the data subject.[131] The processing of personal information contrary to a reasonable expectation of the data subject would constitute an invasion of privacy. Further guidance may be sought in the types of 'internal' processing operations that are recognised by US data protection laws, including necessary security- and fraud-prevention measures and debugging and product enhancement measures. Section 44(1) of POPIA provides a strong indication that the provision should be interpreted in this way, as it refers to the social interests that compete with privacy as including 'the general desirability of the free flow of information' and the 'legitimate interest or public and private bodies in achieving their objectives in an efficient way'.[132] The app developer is thus not required to prove that consent has been given for 'internal operations' of the kind that may reasonably be expected to be performed by a service of that kind. However, direct marketing and the linking of personal information with information held by third parties is strictly regulated by POPIA and would not fall within the scope of legitimate interests.

As is the case under GDPR, where consent is obtained for certain purposes, personal information can also be processed for further purposes, either by obtaining fresh consent for the new purpose,[133] or without consent, provided those further purposes are

---

[131] GDPR rec 47. Processing contrary to the reasonable expectations of a data subject might be an infringement both the right to respect for private and family life and the right to data protection, enshrined in arts 7 & 8 of the Charter of Fundamental Rights of The European Union (2000/C 364/01). Also see the right to respect for private and family life in the Convention for the Protection of Human Rights and Fundamental
Freedoms (European Convention on Human Rights, as amended) (ECHR) ETS 5, 213 UNTS 221 and the right to privacy in s 14 of the Constitution of the Republic of South Africa, 1996. The US constitution does not enshrine a separate right of privacy outside of the protection against unreasonable search and seizure by governments. A right to privacy was introduced into the California Constitution.

[132] POPIA s 44(1)(b).

[133] Ibid s 13(1) makes it clear that consent can only be obtained for a 'specific, explicitly defined and lawful purpose'. Thus any purpose not covered by the original consent, or compatible with the original purposes, requires fresh consent after notice of the new purpose.

'compatible' with the original purpose.[134] POPIA does not, however, require notice to be given to the data subject about this further processing.[135]

Furthermore, there is no provision in South African law comparable to article 5(3) of the EU's e-Privacy Directive.[136] Therefore, these additional grounds of processing may be relied upon by mobile app developers in relation to accessing information on, and storing information to, a user's device.[137]

(g) Notice

POPIA stipulates in some detail the information that must be provided in the notice to the data subject,[138] including:

1. what personal information is being collected and the source from which it is collected;[139]
2. the name and address of the responsible party;[140]
3. the purpose for which the personal information is being collected;[141]
4. whether it is mandatory to provide the personal information to use the service and the consequences of not doing so;[142]

---

[134] Ibid s 15(1). Although POPIA lacks any particularity about what purposes are 'compatible' the factors listed in GDPR art 6(4) ought to be instructive. It is submitted that the provisions of POPIA in relation to linking personal information, special personal information and the information of children make it clear that extra caution should be applied and that as a matter of best practice fresh consent should always be sought.

[135] POPIA s 18(1)(d) read with s 18(2) requires notice to be given before the information is collected of, inter alia, the purpose for which the information is collected. Cf GDPR art 13(3) & art 14(4) which provides: 'Where the controller intends to further process the personal data for a purpose other than that for which the personal data were collected, the controller shall *provide the data subject prior to that further processing with information on that other purpose* and with any relevant further information as referred to in paragraph 2.' (own emphasis).

[136] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector 2002/58/EC (e-Privacy Directive) OJ L 201/37, 31.7.2002.

[137] Save insofar as communication content and metadata is protected by the more limited provisions of the Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 of 2002 (RICA), discussed below.

[138] It goes beyond the provisions of Data Protection Directive 95/46/ECand provides a similar level of protection to GDPR.

[139] POPIA s 18(1)(a). cf GDPR art 14(2)(f). Both cover the source of publically available information.

[140] POPIA s 18(1)(b).

[141] Ibid s 18(1)(c). cf GDPR art 13(1)(c) & (d), and art 14(1)(c) & 14(2)(b), which stipulates that notice must specify any legitimate interests relied upon.

[142] POPIA s 18(1)(d) & (e). Cf GDPR art 13(2)(e).

5. whether information will be transferred to a third country or international organisation (and the level of protection offered);[143]
6. where information is shared, the nature or category of information and the categories of recipients;[144] and
7. the data subject's rights.[145]

Section 18(1) is not a closed list. To comply with the requirement of reasonableness (that is, fairness to the data subject), further information may need to be disclosed.[146] Thus, although POPIA does not require information about how long information will be stored,[147] this would clearly be required if consent were being sought to store information for any longer than would be necessary for achieving the purpose of processing.[148] Furthermore, if the personal information were to be used for profiling or automated-decision making about the data subject, the data subject would have to be given 'sufficient information' about the logic employed by the artificial intelligence (AI) system, and the impact such decisions might have on the data subject.[149]

POPIA does not stipulate the modality by which notice must be given, but does require that 'reasonably practicable steps' be taken by the responsible party to 'ensure that the data subject is aware' of the contents of the notice.[150] This may imply a requirement that the form and wording of the notice have to be such that the data subject can be reasonably expected to understand the contents.

---

[143] POPIA s 18(1)(g) read with chapter 9. Cf GDPR art 13(1)(f) & 14(1)(f) read with Chapter V. Although 'international organisation' is not defined in POPIA it would appear to mean an organisation constituted under public international law and not a multi-national for-profit company. See GDPR art 4(26).
[144] POPIA s 18(1)(h)(i) & (ii).
[145] Ibid s 18(1)(h)(iii)-(v), namely the rights to access and rectify personal information, the right to object to processing and the right to complain to the Information Regulator (and how to do so). The data subject's right of access to personal information is subject to the grounds upon which a responsible party may or must refuse access in terms of Chapter 4 of Part 2 and Chapter 4 of Part 3 of PAIA. The form of the request is governed by s 18 and s 53 of PAIA.
[146] Ibid s 18(1)(h) contains a catch-all that the notice must supply 'any further information … which is necessary, having regard to the specific circumstances in which the information is or is not to be processed, to enable processing in respect of the data subject to be reasonable.'
[147] GDPR art 13(2)(a) & art 14(2)(a). If it is impossible to state an exact period, the data subject must be informed of the criteria that will be applied in determining how long to store personal information.
[148] POPIA s 14(1)(d).
[149] Ibid s 71(3)(b). Cf GDPR art 13(2)(f) & art 14(2)(g) read with art 22.
[150] POPIA s 18(1).

There is no express requirement that the notice be in writing, although this would be advisable to facilitate proof by the responsible party that it has complied with its obligations, including the requirement that it document all processing operations.[151] Unlike GDPR, there is no relaxation of this record-keeping requirement for small entities involved in low-risk processing.[152]

Further notice must be given before personal information is collected from the data subject,[153] and 'as soon as reasonably practicable' after collection in other cases.[154] Notice will cover subsequent collection from the data subject of information of the same kind but only for the same purpose.[155]

These provisions are very similar to the provisions of GDPR,[156] save that there is no requirement for a 'just-in-time' style of notice to be given at the time of collection.[157] POPIA also does not expressly regulate the requirement for online services and websites to have a privacy policy. However, given the requirement to take 'reasonably practicable steps' to ensure that the data subject is aware of the contents of the notice before information is collected from them through a mobile app, it would be advisable to follow best practice adopted in the US and EU, discussed earlier.

What POPIA does require is that a private body, such as a South African mobile app developer, must include information about its processing of personal information in its

---

[151] Ibid s 17.

[152] Ibid s 109(3) does however provide for a number of mitigating factors to be considered in relation to the amount of administrative fine payable for an infringement of the Act, including the nature of the personal information, the number of data subjects affected, and 'the likelihood of substantial damage or distress' to data subjects. Further the Information Regulators powers and functions provide opportunities for education, consultation with industry, and investigations and enforcement notices, before sanctions need to be considered. Cf GDPR art 30(5) which exempts organisations with fewer than 250 employees from the record-keeping requirement. This exemption does not apply however if the processing is likely to pose a risk to the rights and fundamental freedoms of data subjects, is not occasional or involves special personal information or criminal records. Also compare the FTC proposal to exclude entities from its privacy by design framework based on whether they process only non-sensitive data with fewer than 5000 data subjects. In effect, in all three jurisdictions, regulatory tools exist to provide support for SMMEs and ensure that regulatory compliance is not unduly burdensome.

[153] POPIA s 18(2)(a).

[154] Ibid s 18(2)(b).

[155] Ibid s 18(3) provides: 'A responsible party that has previously taken the steps referred to in subsection (1) complies with subsection (1) in relation to the subsequent collection from the data subject of the same information or information of the same kind if the purpose of collection of the information remains the same.'

[156] Cf GDPR art 14, art 15(1)(g), and rec 61. However, GDPR makes it clear that notice must also be given before any further processing commences and before any data is transferred to a third party.

[157] POPIA refers to notice 'before' collection whereas GDPR art 13 and 14 require notice 'at the time when personal data are obtained'. Under POPIA notice in a privacy policy available before download could suffice, whereas GDPR would require the notice to be given when the mobile app first collects the information.

PAIA manual. Section 110 of POPIA amends PAIA, inter alia, by inserting section 51(3). This new section will become operative on 30 June 2021,[158] and will require a responsible party to include the following information in its PAIA manual:

'(c) insofar as the Protection of Personal Information Act, 2013, is concerned-

(i) the purpose of the processing;

(ii) a description of the categories of data subjects and of the information or categories of information relating thereto;

(iii) the recipients or categories of recipients to whom the personal information may be supplied;

(iv) planned transborder flows of personal information; and

(v) a general description allowing a preliminary assessment of the suitability of the information security measures to be implemented by the responsible party to ensure the confidentiality, integrity and availability of the information which is to be processed.'

However, POPIA provides wide exceptions for the delivery of the notice, which go beyond what is included in either US or EU law. Section 18(4) provides:

'(4) It is not necessary for a responsible party to comply with subsection (1) if-

(a) the data subject or a competent person where the data subject is a child has provided consent for the non-compliance;

(b) non-compliance would not prejudice the legitimate interests of the data subject as set out in terms of this Act;

(c) non-compliance is necessary-

(i) to avoid prejudice to the maintenance of the law by any public body, including the prevention, detection, investigation, prosecution and punishment of offences;

(ii) to comply with an obligation imposed by law or to enforce legislation concerning the collection of revenue as defined in section 1 of the South African Revenue Service Act, 1997 (Act 34 of 1997);

[158] Proc R21 *GG* 43461 of 22 June 2020.

(iii) for the conduct of proceedings in any court or tribunal that have been commenced or are reasonably contemplated; or

(iv) In the interests of national security;

(d) compliance would prejudice a lawful purpose of the collection;

(e) compliance is not reasonably practicable in the circumstances of the particular case; or

(f) the information will–

(i) not be used in a form in which the data subject may be identified; or

(ii) be used for historical, statistical or research purposes.'

While subsections (c)(i)–(iv) are consistent with the exclusions in sections 6(1)(c) and the justifications for processing in section 11(1)(c) and (e), the provisions in the remaining sections are problematic.[159]

V ACCOUNTABILITY

POPIA provides in section 8 that the responsible party is accountable for ensuring that all conditions for lawful processing are complied with. The provision of accountability draws upon the 1980 OECD Guidelines, and is now also reflected in GDPR.[160] It provides that the responsible party is accountable not only for its own conduct, but for any processing that is undertaken by others on its behalf. Although no express provision to this effect was included in the 1995 Data Protection Directive, or the US laws considered earlier, such accountability was implied.[161] Crucially, however, the express accountability clause goes further than this and requires the responsible party to take steps to ensure that parties to whom it transfers personal information do not process that information in an unlawful manner.

---

[159] This is further discussed in relation to the amendments proposed in chapter 9.

[160] GDPR art 5(2) provides: 'The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability').'

[161] Data Protection Directive 95/46/ECrec 18 referred to the responsibility of a data controller as follows:
'Whereas, in order to ensure that individuals are not deprived of the protection to which they are entitled under this directive, any processing of personal data in the Community must be carried out in accordance with the law of one of the Member States; whereas, in this connection, processing carried out *under the responsibility of a controller* who is established in a Member State should be governed by the law of that State;' (own emphasis).

In relation to security, POPIA details that the responsible party must take 'reasonable measures[162] to identify security risks both from within[163] and outside the organisation.[164] The responsible party is required to implement and maintain safeguards, which must be regularly verified as effective and kept up to date,[165] in accordance with 'generally accepted information security processes and industry standards'.[166] When there is reason to believe that a data breach has occurred, the responsible party must notify the Regulator and, where possible, the data subject.[167]

To be effective, this obligation must apply whether the data breach occurred while the personal information was being processed by the responsible party, or an operator (or sub-operator). POPIA requires an operator or a sub-operator to process information 'only with the knowledge or authorisation of the responsible party',[168] to keep it confidential, and not to disclose it.[169] The scope of processing permitted is thus limited by the terms of the contract or mandate between the operator and the responsible party. POPIA does not directly impose a duty on the operator (or sub-operator) with regard to security safeguards – the establishment and maintenance of 'appropriate and reasonable technical and organisational

---

[162] POPIA s 19(2).

[163] An example of in internal risk would be a rogue employee who unlawfully access personal information, but could also include negligence by employees, facilitated by lax access controls, insecure passwords or encryption protocols or lack of adequate training in the protection of personal information.

[164] External risks could refer both to hackers targeting the responsible party's information systems, or to risks inherent to the operations of a service provider. POPIA s 19(2) provides: 'In order to give effect to subsection (1), the responsible party must take reasonable measures to-

(a) identify all reasonably foreseeable internal and external risks to personal information in its possession or under its control.' When information is processed by an 'operator' pursuant to a contract, the operator does not by definition fall under the direct control of the responsible party. However it may be argued that the personal information nevertheless remains under the control of the responsible party, as the operator is processing it in terms of a contract with, or mandate from, the responsible party and on its behalf.

[165] Ibid s 19(2)(b)-(d) requires the responsible party to:

'(b) establish and maintain appropriate safeguards against the risks identified;

(c) regularly verify that the safeguards are effectively implemented; and

(d) ensure that the safeguards are continually updated in response to new risks or deficiencies in previously implemented safeguards.'

[166] Ibid s 19(3) provides: 'The responsible party must have due regard to generally accepted information security practices and procedures which may apply to it generally or be required in terms of specific industry or professional rules and regulations.'

[167] Ibid s 22.

[168] Ibid s 20.

[169] Ibid. The section provides: 'Information processed by operator or person acting under authority

An operator or anyone processing personal information on behalf of a responsible party or an operator, must-

(a) process such information only with the knowledge or authorisation of the responsible party; and

(b) treat personal information which comes to their knowledge as confidential and must not disclose it, unless required by law or in the course of the proper performance of their duties.'

measures' required by section 19 will be governed by the terms of the contract or mandate between the operator and the responsible party.[170] The operator must notify the responsible party 'immediately' of a security breach.[171] Where the operator has appointed a sub-operator it must seek suitable contractual safeguards from the sub-operator. In such an instance the operator would be liable for failure to notify the responsible party of the breach.[172]

Although POPIA contains no provision for mandatory data protection impact assessments, these are widely regarded as good practice, and it is difficult to see how a responsible party could comply with its obligation to 'explicitly define' the purposes of processing,[173] and 'identify all reasonably foreseeable internal and external risks to personal information in its possession or under its control'[174] without doing some form of risk assessment. Moreover, the fact that a risk assessment has not been carried out or that good policies, procedures and practices have not been followed is an aggravating factor that may be considered in connection with the imposition of administrative fines.[175] Arguably, the provisions of GDPR which require only a data protection impact assessment and prior consultation with supervisory authorities for 'high risk' processing[176] introduce an element of uncertainty that may obfuscate rather than clarify the law to the detriment of SMMEs.[177] On the other hand, section 57(1), read with section 58, of POPIA sets out an absolute requirement for a responsible party to notify the Information Regulator and obtain prior authorisation before carrying out the following types of processing:

> *'(a) process any unique identifiers of data subjects-*

---

[170] Ibid s 21(1) provides: 'A responsible party must, in terms of a written contract between the responsible party and the operator, ensure that the operator which processes personal information for the responsible party establishes and maintains the security measures referred to in section 19.'
[171] Ibid s 21(2).
[172] This is not expressly provided in POPIA but follows by necessary implication from ss 20 and 21.
[173] POPIA s 13(1). Implied this process must be done systematically and be reviewed periodically so that if the purpose of processing changes, the necessary steps can be taken to ensure that processing remains lawful.
[174] Ibid s 19(2)(b). This process must be done systematically in accordance with industry standards, as 'appropriate safeguards', regular verification, and continual updating of the measures in response to new risks and identified deficiencies in existing safeguards are all expressly required by the Act.
[175] Ibid s 109(3)(g).
[176] GDPR.
[177] Ibid rec 13 indicates that measures were put in place to lower the regulatory burden for SMMEs. However in reality a risk assessment still has to be undertaken.

(i) for a purpose other than the one for which the identifier was specifically intended at collection; and

(ii) with the aim of linking the information together with information processed by other responsible parties;

(b) process information on criminal behaviour or on unlawful or objectionable conduct on behalf of third parties;

(c) process information for the purposes of credit reporting; or

(d) transfer special personal information, as referred to in section 26, or the personal information of children as referred to in section 34, to a third party in a foreign country that does not provide an adequate level of protection for the processing of personal information as referred to in section 72.'

Read with section 71, this provision will provide a powerful handbrake upon the widespread use of targeted advertising, as well as the use of personal information in relation to decisions about employment, credit, insurance, access to other financial products or services and health.[178] Section 71(1) generally prohibits the use of 'automated processing'[179] to create a profile[180] of any data subject as the *sole basis* for a decision imposing legal consequences or some other *substantial* effect upon the data subject.[181] The potentially wide reach of the section, which would cover the kind of profiling based on location, preferences and online conduct used for targeted advertising, is curtailed by these two qualifiers. Arguably, advertising still falls within the net. As explained in chapter 2, ad networks and ad exchanges use algorithms to

---

[178] POPIA s 40(1)(b)(ix)(bb) read with s 44(2) will similarly bring information matching programs by public bodies under the scrutiny of the Information Regulator.

[179] 'Processing', as discussed earlier in this chapter, is a wide term which for the purposes of s 71(1) includes any use, merging or linking of personal information. The term 'automated means' is defined in section 3, for the purposes of that section which defines the application of the Act) as 'any equipment capable of operating automatically in respect to instructions given for the purpose of processing information.' All forms of computerised algorithms, and artificial intelligence or machine learning, used to merge databases, link information across data bases, and identify patterns or create profiles would thus constitute 'automated processing'.

[180] The term 'profile' is not defined, but as discussed in POPIA, targeted advertising is based on recording interests by linking a user's activity (including types of apps downloaded, adverts viewed or clicked, browser search terms, social media activity, and location) to advertiser derived 'interest' lists. Section 71 does not restrict the term, but provides some examples, namely 'performance at work, or his, her or its credit-worthiness, reliability, *location*, health, *personal preferences* or *conduct*.' (own emphasis).

[181] POPIA s 71(1) reads: 'Subject to subsection (2), a data subject may not be subject to a decision which results in legal consequences for him, her or it, or which affects him, her or it to a substantial degree, which is based solely on the basis of the automated processing of personal information intended to provide a profile of such person including his or her performance at work, or his, her or its credit worthiness, reliability, location, health, personal preferences or conduct.

match the ad impressions displayed to a user by linking the unique identifier of the device to a profile of 'interests'. Whether the potentially intrusive nature of highly targeted advertising will substantially affect the user is a matter of interpretation. It is submitted that given the invasion of privacy, particularly when advertisers collect sensitive data such as location, or could infer 'special' personal information such as health status or opinions, their activities must be regarded as having a substantial effect. Since such advertising is not regulated in terms of a contract with the data subject,[182] it will be imperative for the online advertising industry, and stakeholders such as mobile app developers who rely on advertising income, to engage the Information Regulator in consultation, and make application under section 61(1)(b) for the approval of a code of conduct regulating online advertising.[183]

This is an important provision as POPIA, like GDPR, does not expressly provide that if the third party intends to on-sell the information or use it for other purposes, it would be unlawful to transfer the personal information to the third party unless the data subject has been informed of those purposes.[184] However, if the prior authorisation of the Information Regulator is required, an investigation can be conducted, and a statement concerning the lawfulness of processing can be issued.[185] If the Regulator finds that the data subject has not been adequately informed of the purpose of processing (which is thus unlawful), the statement can set out specified steps to be taken in a specified timeframe (or can direct that processing stop).[186]

Chapter 9, which deals with transborder information flows, sets out additional requirements that apply before the responsible party may transfer personal information to 'a

---

[182] Section 71(2)(a) makes provision for an exception to the prohibition where adequate safeguards are included in a contract with the data subject. Section 71(2)(b) makes provision for an exception to the prohibition where the decision 'is governed by a law or code of conduct in which appropriate measures are specified for protecting the legitimate interests of data subjects.'

[183] Chapter 7 governs codes of conduct. Section 60(1) empowers the Information Regulate to issue a code of conduct. In terms of section 61 it may do so either on its own initiative (but after consultation with affected stakeholders or representative bodies) or on application by any body sufficiently representing (in the opinion of the regulator) the industry, profession or vocation that will be regulated by the code. The application must be made in the prescribed form, being Form 3 of the Regulations relating to the Protection of Personal Information in R 1383 *GG* 42110 of 14 December 2018.

[184] The California Consumer Privacy Act of 2018, Cal. Civ. Code §§ 1798.100–1798.199 (CCPA) §1798.115(d) provides expressly that if a third party will on-sell personal information the consumer must have received explicit notice (of the further sale) and been given the right to opt-out provided in §1708.120.

[185] POPIA s 58(5).

[186] Ibid s 95(1)(a) & (b) empowers the Information Regulator to adopt these measures in an enforcement notice. S 58(6) provides that the Information Regulator's statement issued after an investigation into a request for prior authorisation is the equivalent of an enforcement notice in terms of s 95 of the Act.

third party who is in a foreign country'.[187] The provisions require a responsible party to determine whether the law of that country or binding corporate rules between it and the third party provide 'adequate' protection for the protection of the personal information.[188] It is submitted that as 'third party' is not defined in the Act, in this context it must be read as including a transfer to an operator or sub-operator in a foreign country.

Since the definition of responsible party admits for multiple responsible parties (who may act alone or in conjunction with others), in the situation where a third party received personal information for processing, it would itself be a responsible party, and must give notice to the data subject of its operations (unless the data subject is already 'aware' of the information.)[189]

VI DATA MINIMISATION

The data minimisation principle contained in section 10 restricts the collection of information beyond what is 'adequate, relevant and not excessive' for the purpose for which it is processed. This would ordinarily mean the purpose(s) specified in the notice to the data subject, provided that if the notice refers to multiple purposes, it is clear what kinds of information will be processed for each purpose.

As discussed in relation to US and EU law, this principle does not in fact impose a condition that collection is kept to a strict minimum, because with the consent of the data subject, personal information can be collected for any specified purpose, even if that purpose is not strictly necessary for the performance of the contract, or the provision of the service requested by the data subject.

Section 14 imposes a storage limitation, in that a record of personal information may not be retained beyond the period that is 'necessary' for the specific purpose for which it was collected or subsequently processed.[190] The storage period may also be imposed by law or

---

[187] Ibid s 72(1).
[188] Ibid.
[189] Ibid s 18(2)(a). The term is regrettably vague. It is submitted that this should be interpreted to require that notice given to the data subject sets out specifically and explicitly the personal information, the purpose of processing, and the further information about the identity of the responsible party and other disclosures required. It is not sufficient to argue that a data subject is generally 'aware' that reference to 'advertising' in a privacy policy means that third party ad networks will receive and process his or her personal information.
[190] Ibid s 14 Retention and restriction of records:

an applicable code.[191] Information must be destroyed, deleted or de-identified 'as soon as reasonably practicable' after it is no longer necessary to retain it.[192] If personal information is being processed unlawfully, it would ordinarily need to be destroyed or deleted, but in certain instances, processing can be 'restricted' on notice or in accordance with instructions from the data subject, for example, to verify the accuracy of the data.[193]

POPIA includes an exception to the storage limitation where personal information is retained for 'historical, statistical and research purposes'.[194] This exception is more widely framed than either article 6(1)(b) of the 1995 Data Protection Directive[195] or article 5(1)(b) of GDPR.[196] Arguably, the collection of statistics derived from app analytics and the use of app data for market research and product development could be exempt from the storage limitation and not subject to mandatory de-identification of the data. On the contrary,

---

'14(1) Subject to subsections (2) and (3), records of personal information must not be retained any longer than is necessary for achieving the purpose for which the information was collected or subsequently processed, unless–
(a) retention of the record is required or authorised by law;
(b) the responsible party reasonably requires the record for lawful purposes related to its functions or activities;
(c) retention of the record is required by a contract between the parties thereto; or
(d) the data subject or a competent person where the data subject is a child has consented to the retention of the record.'

[191] Section 14(3). 'A responsible party that has used a record of personal information of a data subject to make a decision about the data subject, must–
(a) retain the record for such period as may be required or prescribed by law or a code of conduct; or
(b) if there is no law or code of conduct prescribing a retention period, retain the record for a period which will afford the data subject a reasonable opportunity,
taking all considerations relating to the use of the personal information into account, to request access to the record.'

[192] Section 14(4): 'A responsible party must destroy or delete a record of personal information or de-identify it as soon as reasonably practicable after the responsible party is no longer authorised to retain the record in terms of subsection (1) or (2).' Information can only be regarded as 'de-identified' [as defined] if it cannot reasonably be re-identified. Thus s 14(5) provides that '[t]he destruction or deletion of a record of personal information in terms of subsection (4) must be done in a manner that prevents its reconstruction in an intelligible form.'

[193] POPIA s 14(5) – (8).

[194] Section 14(2): 'Records of personal information may be retained for periods in excess of those contemplated in subsection (1) for historical, statistical or research purposes if the responsible party has established appropriate safeguards against the records being used for any other purposes.'

[195] Data Protection Directive 95/46/ECart 6(1)(b): 'collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible provided that Member States provide appropriate safeguards.'

[196] GDPR art 5(1)(b) provides that 'further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes.' Art 89(1), read with rec 156, requires such processing to be subject to 'appropriate safeguards' and in accordance with the principle of data minimisation. The controller must anonymise the data, unless this is not feasible, in which case appropriate safeguards should be applied such as pseudonymising the data.

under GDPR, 'anonymous data' can be used for statistical and research purposes.[197] Personal information (subject to safeguards such as pseudonymisation) can be used for the more limited purposes of 'archiving purposes in the public interest, scientific or historical research purposes or statistical purposes'.[198]

Furthermore, consent is not the only basis upon which personal information can be processed for statistical and research purposes. Section 15(1) permits further processing of personal information if the purpose of such further processing is 'compatible' with the purpose of collection. While there is a range of objective factors that must be considered in making such a determination,[199] POPIA also contains a deeming provision in terms of which a number of grounds will be regarded as the basis for 'compatible' further processing.[200] These include where 'the information is used for historical, statistical or research purposes and the responsible party ensures that the further processing is carried out solely for such purposes and will not be published in an identifiable form'.[201]

VII THE SUPPORTING STATUTORY FRAMEWORK FOR e-PRIVACY

South Africa does not have a comprehensive e-Privacy statute, but a number of disparate statutes (each with a different scope of application) could apply to mobile applications. Only those aspects relevant to the protection of personal information will be considered below.

---

[197] Ibid rec 26 provides: 'The principles of data protection should therefore not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable. This Regulation does not therefore concern the processing of such anonymous information, including for statistical or research purposes.'

[198] Ibid art 5(1)(b).

[199] POPIA s 15(2) provides: 'To assess whether further processing is compatible with the purpose of–

(a) the relationship between the purpose of the intended further processing and the purpose for which the information has been collected;
(b) the nature of the information concerned;
(c) the consequences of the intended further processing for the data subject;
(d) the manner in which the information has been collected; and
(e) any contractual rights and obligations between the parties.'

[200] Ibid s 15(3). In relation to private bodies the most frequently relied upon grounds would likely be data subject consent for the further processing, and necessity to comply with a legal obligation. The Information Regulator can exempt processing activities in terms of section 37, inter alia, if a 'clear benefit' to the data subject and/or a third party outweighs 'to a substantial degree' any privacy infringement.

[201] Ibid s 15(3)(e).

(a) Promotion of Access to Information Act 2 of 2000 (PAIA)

The requirement to document processing operations[202] must be read with section 51 of PAIA, which sets out the requirement of a private body[203] to publish a PAIA manual, which must, inter alia, provide information about the processing of personal information. Section 110 read with the Schedule to POPIA substitutes the definition of 'personal information' in PAIA.[204]

In addition to the information about how to access information held by the private body,[205] a PAIA manual will be required to set out in relation to personal information:

> *'(i) the purpose of the processing;*
>
> *(ii) a description of the categories of data subjects and of the information or categories of information relating thereto;*
>
> *(iii) the recipients or categories of recipients to whom the personal information may be supplied;*
>
> *(iv) planned transborder flows of personal information; and*
>
> *(v) a general description allowing a preliminary assessment of the suitability of the information security measures to be implemented by the responsible party to ensure the confidentiality, integrity and availability of the information which is to be processed.'*[206]

All mobile app developers, regardless of their form (or lack) of corporate structure, fall within the definition of a 'private body' for the purposes of PAIA.[207] The exemption from the requirement to publish a PAIA manual which was promulgated in favour of small entities will

---

[202] Ibid s 17.
[203] This would include a mobile app developer. The consideration of the processing of personal information by public bodies, including mobile apps developed by such public bodies, and other e-government services, is beyond the scope of this dissertation.
[204] Save that under POPIA personal information relates to a 'living' natural person, whereas under PAIA, personal information will include information about an individual who has been dead for not more than 20 years. Unlike POPIA, PAIA has no application to information about juristic persons.
[205] PAIA s 10, read with s 51(1)(a) & (b).
[206] Ibid s 51(1)(c)(i)-(v).
[207] Ibid s 1. The term 'private body' is defined to include natural persons in the course of carrying on their profession, trade or business, partnerships and juristic persons, such as companies.

end on 20 December 2020.[208] Thereafter, each mobile app developer in South Africa[209] must produce such a manual. The manual must be made available on its website (if any), as well as at its principal place of business, and on request, to the Information Regulator or any other person.[210]

The requirement to appoint an 'information officer' under section 55 of POPIA applies to all public and private bodies, and the provisions of section 17 of PAIA (in relation to the appointment of deputy information officers) must be read as applying mutatis mutandis to private bodies.[211] Thus, the app developer him- or herself or, in the case of a corporate entity, the CEO or an employee designated to act as information officer or deputy information officer, must be identified in the PAIA manual, and contact details of such person must be supplied for the purposes of receiving requests and complaints regarding access to information.[212] Unlike GDPR, there is no exemption from the requirement for an information officer for entities involved in small-scale processing of non-sensitive information.[213]

PAIA will apply to any 'record'[214] of information (including but not limited to 'personal information') held by a mobile app developer, whether or not the information was created by the app developer. If information is held by an independent subcontractor (which would include any 'operator' (as defined in POPIA) who is appointed to process personal information), it is deemed to be held by the app developer.[215]

---

[208] Promotion of Access to Information Act, 2000 (Act No.2 Of 2000) Exemption Of Certain Private Bodies From Compiling Manual in GN 1222 *GG* 39504 of 11 December 2015. The exemption applied to all private bodies except public companies, and private companies, as defined in s 1 of the Companies Act 71 of 2008, with 50 or more employees, or an annual turnover equal to or exceeding R30 million (in the transport, storage and communications sector applicable to IT companies).

[209] PAIA is not expressly extra-territorial. A full consideration of whether its provisions are enforceable against foreign mobile app developers holding records of personal information about South Africans is beyond the scope of this dissertation, but prima facie there would be difficulties in establishing jurisdiction and enforcing compliance in such instances.

[210] Ibid s 51(3).

[211] POPIA s 56, read with PAIA s 17.

[212] PAIA s 1, definition of 'head' read with s 51(1)(a) which requires a postal and street address, phone number, fax number and (if available) an email address to be supplied for the 'head' of a private body, i.e. the 'information officer' as required by POPIA.

[213] cf GDPR s 37(1)(b) and (c).

[214] PAIA s 1. The term 'record' is defined as 'any recorded information-

(a) regardless of form or medium;
(b) in the possession or under the control of that public or private body, respectively; and
(c) whether or not it was created by that public or private body, respectively'.

[215] Ibid s 4 provides that '[f]or the purposes of this Act, ... a record in the possession or under the control of-

(a) an official of a public body or private body in his or her capacity as such; or
(b) an independent contractor engaged by a public body or private body in the capacity as such contractor,

As PAIA's objective is primarily to facilitate the constitutional right of access to information,[216] which may at times conflict with an individual's right to privacy, PAIA will play a key role in determining when access to personal information may or must be refused,[217] internal dispute resolution processes,[218] complaints to and investigations by the Information Regulator,[219] and resort to the courts.[220] Guidance on how to balance these competing interests within South Africa's constitutional dispensation is an important area for future research.

(b) Electronic Communications Act 36 of 2005 (ECA)

The ECA defines a number of key concepts. An electronic communications service[221] would thus include any mobile app that conveys communications such as VOIP, messaging or video calling. It would exclude content-services[222] and streaming services (which may be classified as either content-services or 'broadcasting'[223]). It would also exclude all mobile apps that do not have a communication functionality.

The mobile app owner is the electronic communications service provider. When the mobile app transfers communications via the internet through a Wi-Fi network or cellular network, it is using an electronic communications network.[224] The internet service provider

---

is regarded as being a record of that public body or private body, respectively'.

[216] Constitution of the Republic of South Africa, 1996 s 32.

[217] PAIA. In relation to records held by private bodies see part 3, s 61 (in relation to health records) and chapter 4 (ss 62–70).

[218] Ibid. See part 4, chapter 2 (ss 74–77).

[219] Ibid s 77A–77K (inserted by POPIA).

[220] Ibid s 78 (as amended by POPIA).

[221] ECA s 1 defines 'electronic communications service' as 'any service provided to the public, sections of the public, the State, or the subscribers to such service, which consists wholly or mainly of the conveyance by any means of electronic communications over an electronic communications network, but excludes broadcasting services.'

[222] The term is not defined.

[223] ECA s 1. The term 'broadcasting' is defined as 'any form of unidirectional electronic communications intended for reception by–

(a) the public;

(b) sections of the public; or

(c) subscribers to any broadcasting service,

whether conveyed by means of radio frequency spectrum or any electronic communications network or any combination thereof, and 'broadcast' is construed accordingly;'.

[224] Ibid. The term 'electronic communications' is defined as 'the emission, transmission or reception of information, including without limitation, voice, sound, data, text, video, animation, visual images, moving images and pictures, signals or a combination thereof by means of magnetism, radio or other electromagnetic waves, optical, electromagnetic systems or any agency of a like nature, whether with or without the aid of tangible conduct, but does not include content service;'.

and the cellular carrier would be electronic communications network service providers and must be licensed under the Act.[225]

(c) Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 of 2002 (RICA)

RICA relates to both 'direct' (face-to-face) communication[226] and 'indirect' communication[227] by any 'electronic communications service'.[228] A communication via a mobile app offering an electronic communication service would thus be an 'indirect communication' for the purposes of RICA.

Section 2 of RICA[229] protects the 'contents'[230] of an electronic 'communication'[231] against 'interception'.[232] When a mobile app permits any person other than a participant in the communication to view, examine or inspect the content of the communication, or when it permits recording or listening to the communication by a non-

[225] Ibid s 5(3)(a) requires a network operated for commercial purposes at provincial or national scope (i.e. excluding local area networks) to be licensed. Only voice telephony services operating through the national numbering plan require a licence as an electronic communications service provider in terms of s 5(3)(c).

[226] RICA. The term 'direct communication' is defined as–

'*(a)* oral communication, other than an indirect communication, between two or more persons which occurs in the immediate presence of all the persons participating in that communication; or

(b) utterance by a person who is participating in an indirect communication, if the utterance is audible to another person who, at the time that the indirect communication occurs, is in the immediate presence of the person participating in the indirect communication.'.

[227] Although the term 'indirect communication' is not defined, it is any communication that does not occur directly- that is within the immediate presence of the persons participating in the communication.

[228] RICA s 1. 'Electronic communications service' is defined in RICA as 'means electronic communications service as defined in the ECA.

[229] RICA. Section 2 provides: 'Subject to this Act, no person may intentionally intercept or attempt to intercept, or authorise or procure any other person to intercept or attempt to intercept, at any place in the Republic, any communication in the course of its occurrence or transmission.'

[230] Ibid s 1 provides that '[t]he term "contents", when used with respect to any communication, includes any information concerning the substance, purport or meaning of that communication.'

[231] Ibid s 1. The term 'communication' is defined as including both 'direct communication' and Indirect communication'.

[232] Ibid s 1. The term 'intercept' is defined as 'the aural or other acquisition of the *contents* of any communication through the use of any means, including an interception device, so as to make some or all of the contents of a communication available to a person other than the sender or recipient or intended recipient of that communication, and includes the-

(a) monitoring of any such communication by means of a monitoring device;

(b) viewing, examination or inspection of the contents of any indirect communication; and

(c) diversion of any indirect communication from its intended destination to any other destination, and 'interception' has a corresponding meaning;' (own emphasis).

participant,[233] this would be an unlawful interception unless one of the parties to the communication has given consent,[234] or another lawful ground for interception exists.[235]

In terms of section 30(1) of RICA, an electronic communications service provider must provide a service that is capable of being intercepted and must store communication metadata about the origin, destination, termination, duration and equipment used for every communication made or received by its customer, that is, 'communication-related information'.[236]

The communications-related information held by an 'electronic communications service provider'[237] may not 'intentionally' be supplied to any person (other than the customer) without the written authorisation of the customer on each occasion specifying the person to whom it will be transferred,[238] or another lawful basis, such as an interception directive for law enforcement. [239]

---

[233] Ibid s 1. The term 'monitor' is defined as including 'to listen to or record communications by means of a monitoring device'. The term 'monitoring device' is defined as 'any electronic, mechanical or other instrument, device, equipment or apparatus which is used or can be used, whether by itself or in combination with any other instrument, device, equipment or apparatus, to listen to or record any communication'. This would include a mobile app installed on a mobile device.

[234] Ibid s 5(1) provides: 'Any person, other than a law enforcement officer, may intercept any communication if one of the parties to the communication has given prior consent in writing to such interception, unless such communication is intercepted by such person for purposes of committing an offence.' Consent is not otherwise defined.

[235] Ibid ss 3–9.

[236] Ibid s 1. The term 'communication-related information' is defined as 'any information relating to an indirect communication which is available in the records of a [electronic communications] service provider, and includes switching, dialling or signalling information that identifies the origin, destination, termination, duration, and equipment used in respect, of each indirect communication generated or received by a customer or user of any equipment, facility or service provided by such a [electronic communications] service provider and, where applicable, the location of the user within the [electronic communications] system;'. The ECA s 97 read with the Schedule to the Act substitutes references to a 'telecommunication' service, service provider and system with 'electronic communications' service, service provider, and system.

[237] RICA s 1. The term 'electronic communication service provider' is defined as 'any-

(a) person who provides an electronic communication service under and in accordance with a electronic communication service licence issued to such person under Chapter 3 of the Electronic Communications Act, and includes any person who provides-

(i) a local access communication service, public pay-telephone service, value-added network service or private electronic communication network as defined in the Electronic Communications Act; or

(ii) any other electronic communication service licensed or deemed to be licensed or exempted from being licensed as such in terms of the Electronic Communications Act; and

(b) Internet service provider;'.

[238] Ibid s 14.

[239] Ibid ss 13, 15, 17 & 19.

By virtue of the definition of electronic communications service provider in RICA, this prohibition applies to the 'internet service provider'[240] and to the mobile app owner (even if exempted from licensing under the ECA). It applies to both real-time data (current within 90 days of the communication)[241] and archived data.[242]

However, RICA contains none of the other protections afforded by the e-Privacy Directive in the EU, and in particular has no equivalent of article 5(3), requiring consent to access or store information on the terminal equipment of a subscriber. This lacuna highlights the need for consideration of a sector-specific law capable of adequately regulating the collection of information from, and storage of information to, smart devices by mobile applications.[243]

(d) Electronic Communications and Transactions Act 25 of 2002 (ECTA)

The provisions regulating direct marketing in section 45, and the protection of personal information in sections 50 and 51 of ECTA, will be repealed and replaced by POPIA when that Act comes into operation. In addition, ECTA contains consumer protection provisions relevant to 'electronic transactions'.[244] The installation of a mobile application (even if it is free to download) is an electronic transaction. Section 43 requires comprehensive information to be

[240] Ibid s 1. The term 'internet service provider' is defined as 'any person who provides access to, or any other service related to, the Internet to another person, whether or not such access or service is provided under and in accordance with an electronic communication service licence issued to the first-mentioned person under Chapter 3 of the Electronic Communications Act;'.

[241] Ibid s 1. The term 'real-time communication-related information' is defined as 'communication-related information which is immediately available to a telecommunication service provider-

(a) before, during, or for a period of 90 days after, the transmission of an indirect communication; and

(b) in a manner that allows the communication-related information to be associated with the indirect communication to which it relates.'

[242] Ibid s 1. The term 'archived communication-related information' is defined as 'any communication-related information in the possession of a telecommunication service provider and which is being stored by that telecommunication service provider in terms of section 30 (1) *(b)* for the period determined in a directive referred to in section 30 (2) *(a)*, beginning on the first day immediately following the expiration of a period of 90 days after the date of the transmission of the indirect communication to which that communication-related information relates;'.

[243] The content and form of such law is an area of future study, but lies outside the focus of this dissertation.

[244] Electronic Communications and Transactions Act 25 of 2002 (ECTA) s 42. The term is not defined, but in s 1 a 'transaction' is defined as 'a transaction of either a commercial or non-commercial nature, and includes the provision of information and e-government services.'

supplied to the consumer by the supplier of 'goods'[245] or 'services'[246] offered through an electronic transaction. In the context of mobile apps, the app user would be the 'consumer'[247] and the app owner would be the supplier.[248] The information provided must include the full name, legal status,[249] email address, website, telephone number and physical address of the app owner (that is, the 'supplier').

However, the provisions of section 43 of ECTA do not reconcile neatly with POPIA when applied to the mobile apps ecosystem. First, where the app owner shares data with other parties, such as processors or third parties, there is no indication as to what information must be supplied about these other parties.

Secondly, such information must include:

> *'(h) a sufficient description of the main characteristics of the goods or services offered by that supplier to enable a consumer to make an informed decision on the proposed electronic transaction; [and]*
>
> ...
>
> *(p) the security procedures and privacy policy of that supplier in respect of payment, payment information and personal information;'*[250]

The definition of 'personal information' in POPIA will be substituted for the existing definition.

However, section 43 requires the supplier to 'make the [said] information available to consumers on the web site where such goods or services are offered'. In the context of mobile apps, this may be interpreted to mean that there must be a link to a privacy policy

---

[245] The term is not defined in ECTA. In the CPA the term 'goods' is very widely defined. It includes any kinds of tangible goods (such as might be offered for sale in an e-commerce app) but extends to include in subpara (c) 'any literature, music, photograph, motion picture, game, information, data, software, code or other intangible product written or encoded on any medium, or a licence to use any such intangible product'.

[246] The term is not defined in ECTA. In the CPA the term 'services' is widely defined and includes any provision of 'direct or indirect benefit' to the consumer, including information, education, entertainment and any similar 'intangible' product. This clearly includes all categories of mobile apps.

[247] ECTA s 1. The term 'consumer' is defined as 'any natural person who enters or intends entering into an electronic transaction with a supplier as the end user of the goods or services offered by that supplier'.

[248] The term is not defined in ECTA. In the Consumer Protection Act 68 of 2008 (CPA) s 1 the term 'supplier' is defined as a person who markets any goods or services'.

[249] ECTA s 43(1)(a). Subsec (f) provides further that a legal person such as a company must supply its registration number, the names of its office bearers and its place of registration.

[250] Ibid s 43(1)(h) & (p).

containing this information on the app's website, and in the app store. However, ECTA lacks any provision that the privacy policy must also be posted on the home page of the app or in app settings. Further, it lacks any provision requiring the information to be 'prominent', 'conspicuous' or 'readily accessible'.[251]

Lastly, in relation to security of payment systems, ECTA provides in section 43:

> *'(5) The supplier must utilise a payment system that is sufficiently secure with reference to accepted technological standards at the time of the transaction and the type of transaction concerned.*
>
> *(6) The supplier is liable for any damage suffered by a consumer due to a failure by the supplier to comply with subsection (5).'*

Under POPIA, the security requirement extends beyond payment systems, to include all personal information.

(e) Consumer Protection Act 68 of 2008 (CPA)

While POPIA and ECTA lack any provision requiring the information to be presented in a format and language that is clear and easy to understand, this is required by section 22(1)(b) read with section 22(2) of the CPA insofar as the data subject is a consumer for the purposes of the CPA.[252] Section 22 provides:

> *'Right to information in plain and understandable language*
>
> *(1) The producer of a notice, document or visual representation that is required, in terms of this Act or any other law, to be produced, provided or displayed to a consumer must produce, provide or display that notice, document or visual representation–*
>
> *(a) in the form prescribed in terms of this Act or any other legislation, if any, for that notice, document or visual representation; or*

[251] Compare COPPA, CalOPPA and GDPR.

[252] A consumer as defined in the CPA includes a person to whom goods are marketed or who enters into a transaction in the ordinary course of the supplier's business, and can also include the user of goods or the recipient or beneficiary of services even if they did not enter into the transaction. This would apply to all natural persons but, unlike ECTA, the CPA also includes juristic persons with an asset value or annual turnover below R2 million. Determination of threshold in terms of the Consumer Protection Act, 2008 (Act 68 of 2008) in GN 294 *GG* 34181 of 1 April 2011.

(b) in plain language, if no form has been prescribed for that notice, document or visual representation.

(2) For the purposes of this Act, a notice, document or visual representation is in plain language if it is reasonable to conclude that an ordinary consumer of the class of persons for whom the notice, document or visual representation is intended, with average literacy skills and minimal experience as a consumer of the relevant goods or services, could be expected to understand the content, significance and import of the notice, document or visual representation without undue effort, having regard to–

(a) the context, comprehensiveness and consistency of the notice, document or visual representation;

(b) the organisation, form and style of the notice, document or visual representation;

(c) the vocabulary, usage and sentence structure of the notice, document or visual representation; and

(d) the use of any illustrations, examples, headings or other aids to reading and understanding.'

VIII AN ACCOUNTABILITY GAP?

While POPIA provides strong protection for the processing of personal information by responsible parties, and any 'downstream' processing (as described in chapter 2) by processors, it provides weaker protection in relation to third party processing. Although third parties will be responsible parties in their own right and fully liable under POPIA, the enforceability of those obligations is considerably weakened if the data subject remains unaware of their activities. Presently the onus is placed a data subject to exercise their right under section 23(1)(b) of POPIA to request that the app developer provide them with the identity of all third parties who have, or have had, access to their personal information. The app developer could comply with the section by providing only the 'category' of third parties. Simply put the data subject with no user-friendly information about the identity, location, contact details, and processing activities undertaken by third parties is unable to ensure that their personal data is being processed lawfully.

Furthermore, as with the US and EU laws discussed earlier, there is an 'accountability gap' in POPIA, in that it does not apply directly to a party that is not a 'responsible party' or a 'processor' in relation to the collection of personal information, namely

hardware manufacturers, OS manufacturers, SDK and API developers and platforms such as app stores and content services (like YouTube). These 'gatekeeper' parties may play a decisive role in determining the means of processing through the provision of APIs and SDKs. Some of these entities will be responsible parties insofar as their own processing of personal information is concerned, but they have no accountability if the way their technology or platform is designed or used by others makes it impossible, or difficult to comply with data protection laws (or conversely, if there are no safeguards or it is easy to flout data protection mechanisms).

IX CONCLUSION

Although POPIA does encompass the wider data protection principles that underpin GDPR, and thus goes beyond the FIPPS of notice, consent, access and security, there are certain respects in which sector-specific protections in relation to important areas are lacking.

Firstly COPPA, CalOPPA, CCPA and GDPR all require that conspicuous notice be given of what personal information is collected. POPIA requires notice and informed consent, which would imply a requirement that the notice is clear and complete. When read together with the CPA, there is an express 'plain language' requirement.

POPIA does not afford the same stringent protection to children offered by COPPA. It does not require direct notice to a child's parents, it does not stipulate a right to refuse to consent to the collection for processing that goes beyond the purpose of the service (for example, targeted advertising), and it does not contain any guidance on 'verified' parental consent.[253]

POPIA and RICA also contain no provision that would regulate the collection of information from and storage to smart devices by mobile apps. The provisions of RICA would apply to the collection of content and metadata by mobile apps falling within the definition of 'electronic communications service' but would not cover any other mobile applications. There is a clear need for the development of sector-specific regulation in this regard to provide adequate protection, particularly in relation to information that might not be

[253] The Information Regulator may impose conditions to further regulate these matters under section 35(3)(a)-(d). Thus such conditions could specify when and how notice is to be given to parents, and how parents can refuse to permit 'further processing'.

classified as personal information, but which may still impact upon the privacy of the data subject by accessing their device.

In general, however, POPIA affords strong protection to personal information. Whereas much data collection is unregulated in the US, and whereas CalOPPA and the CCPA generally permit what is termed opt-out consent, POPIA makes all processing of personal information unlawful unless the responsible party can demonstrate that it has received the voluntary, specific and informed consent of the data subject, or there is some other lawful ground for processing the personal information. It has been argued that although POPIA's provisions are less clear than the expanded provisions on consent in GDPR, it is clearly implied from the requirement for voluntary specific and informed consent that POPIA also requires 'opt-in' consent (or some other lawful basis for processing) before any personal information is collected. Default settings configured to permit the collection of any personal information beyond the terms of the consent, save insofar as it was necessary for the provision of the service (or justified on some other ground), would not be lawful.

CHAPTER 7

THE INCLUSION OF 'PRIVACY BY DESIGN' IN REGULATORY GUIDELINES FOR MOBILE APP DEVELOPERS IN THE US

I INTRODUCTION

The rapid development of technology and the new uses for personal data are proving a challenge to the application of privacy laws.[1] This dissertation adopts the conceptual framework of 'Privacy by Design' (PbD) which, as explained in chapter 3, is the

> *'concept of engineering privacy directly into the design of new technologies, business practices and networked infrastructure, in order to achieve the doubly-enabled pairing of functionality and privacy'*.[2]

It is important to recognise that although PbD is not explicitly referred to in data protection legislation (with the notable exception of article 25 of GDPR[3]), it has achieved universal acceptance as the guiding philosophy underpinning data protection laws.

> *'PBD aims at building privacy and data protection up front, into the design specifications and architecture of information and communication systems and technologies, in order to facilitate compliance with privacy and data protection principles.'*[4]

In 2010, the 32nd International Conference of Data Protection and Privacy Commissioners adopted a unanimous resolution on PbD[5] and the concept has continued to grow in popularity.[6]

---

[1] OECD, *The OECD Privacy Framework* (2013) at 66.

[2] A Cavoukian and M Prosch, *The Roadmap for Privacy by Design in Mobile Communications: A Practical Tool For Developers, Service Providers, and Users* (Toronto, ON, Canada: Office of the Privacy Commissioner, Ontario, Canada, 2010) at 3.

[3] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA OJ L 119, 4.5.2016 (EU General Data Protection Regulation; GDPR).

[4] European Data Protection Supervisor (EDPS), 'Glossary 'Privacy by Design'' <https://edps.europa.eu/node/3110#privacy_by_design> accessed 17 February 2020.

[5] *Resolution on Privacy by Design* (Jerusalem, 29 October 2010). Also see A Cavoukian, *Privacy by Design Strong Privacy Protection – Now, and Well into the Future a Report on the State of PbD to 33rd International Conference of Data Protection and Privacy Commissioners* (Toronto, ON, Canada: Office of the Privacy Commissioner, Ontario, Canada, 2011) at 6.

[6] Kirsten Martin and Katie Shilton, 'Putting Mobile Application Privacy in Context: An Empirical Study of User Privacy Expectations For Mobile Devices' (2016) 32 *The Information Society* 200–216 at 201.

This chapter sets out the foundational principles encapsulated in the concept of 'PbD' and discusses the origins of the concept, and the regulatory guidance issued to mobile application developers in the US and other jurisdictions.

The off-spring of PbD is the closely related concept of Privacy by (re)Design (Pb(re)D). Although the foundational principles of PbD remain unchanged, Pb(re)D seeks to go beyond application to *new* technologies, practices and infrastructure, to achieve the *re-design* of existing technologies and systems. In the context of the complex mobile apps ecosystem where app developers are constrained by the existing third party hardware and software, Pb(re)D is particularly appropriate as it recognises that redesigning an ecosystem cannot be achieved without all parties playing a role.

Given the further, considerable complexity introduced by multiple, partially overlapping legislative frameworks for data protection that may all apply to a single mobile application, the analysis in this chapter will extract the key legal issues on which it is necessary to provide clarity for both mobile app developers and regulators if Pb(re)D is to be achieved in the mobile apps ecosystem.

II THE FOUNDATIONAL PRINCIPLES OF PbD

The conceptual framework of PbD comprises seven foundational principles:[7]

1. Privacy measures are proactive not reactive;
2. Privacy is the default setting;
3. Privacy is embedded into design;
4. Privacy is secured alongside full functionality;
5. Privacy is secured across the full data lifecycle;
6. Processing is transparent; and
7. Privacy is user-centric and user-friendly.

[7] A Cavoukian, *Privacy by Design and the Emerging Personal Data Ecosystem* (Toronto, ON, Canada: Office of the Privacy Commissioner, Ontario, Canada, 2012) at 16.

The concept that technology is neutral rather than inherently privacy invasive underpins PbD.[8] Developing technologies that protect privacy can go hand in hand with innovation, security and the legitimate business interests of industry.[9]

Cavoukian asserts that PbD is thus a set of 'information management principles' that reinforce but go beyond the 'universal principles' of the Fair Information Practices (FIPs).[10] As described earlier, while FIPs emerged in the 1970s, and there is broad convergence around core principles, there are divergent approaches to the content of the FIPs, both within and outside the US. The US favours sector-specific legislation and lacks a general federal privacy statute that regulates the use of personal information by the private sector. In the US, the Federal Trade Commission (FTC) has published fair information practice principles (FIPPs) that comprise the four principles of notice, choice, access and security.[11] European Union law places greater emphasis on the principle of data minimisation,[12] data quality and a broader concept of notice that includes notice of a data subject's rights to access and correct personal information held about them.[13]

However, there is an even more significant substantive difference in the core principles adopted in the regimes: in the EU, and under POPIA, data may be processed only if a lawful basis exists for the processing. The US, on the other hand, perhaps in deference to the first amendment right to free speech, permits processing unless a law 'specifically forbids the activity'.[14]

It may be correct for Cavoukian to assert that PbD represents the 'highest global standard possible' and is a 'significant "raising" of the bar' for privacy protection set by the

---

[8] A Cavoukian, 'Privacy by design: The global privacy standard' (16 October 2018) <https://www.standardsuniversity.org/e-magazine/october-2018-volume-9-issue-3-privacy-freedom-human-rights/privacy-by-design-the-global-privacy-standard/> accessed 24 February 2020.

[9] Cavoukian, 'Privacy by design: The global privacy standard'.

[10] A Cavoukian, 'Privacy by Design The 7 Foundational Principles Implementation and Mapping of Fair Information Practices' <https://iab.org/wp-content/IAB-uploads/2011/03/fred_carter.pdf> accessed 17 September 2019

[11] But these are by no means uniformly represented in the various federal and state laws regulating data protection in specific sectors.

[12] Contrasted below with the FTC's approach to 'reasonable collection limits'. Cf Ira S Rubinstein and Nathaniel Good, 'Privacy by Design: A Counterfactual Analysis of Google and Facebook Privacy Incidents' (2013) 28 *Berkeley Tech LJ* 1333–1414 at 1358. The writer asserts that 'data avoidance' and 'data minimization' (used interchangeably, but it is submitted incorrectly so) are 'central tenets' of the FIPPS.

[13] Paul M Schwartz, 'The EU-US Privacy Collision: A Turn to Institutions and Procedures' (2012) 126 *Harv L Rev* 1966–2009 at 1976.

[14] Ibid.

FIPs.[15] However, GDPR and POPIA are not restricted to the FIPs, being based upon earlier and wider data protection principles that provide significantly wider protection that encompasses the principle that data processing may not take place without a lawful basis.[16] The analysis of those principles against the principles of PbD will be undertaken in the chapters which follow.

III PbD IN THE UNITED STATES

The first comprehensive PbD guidelines issued specifically to mobile application developers originated in North America in 2011, in a report authored by Cavoukian and Prosch and published jointly by the Arizona State University's PbD Research Lab and the Information and Privacy Commissioner, Ontario, Canada.[17]

PbD is not referred to in any existing US legislation, nor is it expressly referred to in any of the federal privacy bills introduced in 2019. However, this is not to say that PbD is not applied in the US. On the contrary, some key elements of a PbD approach have always been part of the US approach to data protection. In 1995 a government task force outlined an 'information privacy principle'.[18] In its report, the task team advises:

> 'A critical characteristic of privacy is that once it is lost, it can rarely be restored. … Given this characteristic, privacy should not be addressed as a mere afterthought, once personal information has been acquired. Rather, information users should explicitly consider the impact on privacy *in the very process of designing information systems* and in deciding whether to acquire or use personal information in the first place.'[19] (Own emphasis.)

---

[15] Cavoukian, 'Privacy by Design The 7 Foundational Principles Implementation and Mapping of Fair Information Practices'.

[16] Lee A Bygrave, 'Data Protection by Design and by Default: Deciphering the EU's Legislative Requirements' (2017) 4 *Oslo Law Review* 105–120 makes a similar argument, stating that even though art 25 of GDPR is tethered to compliance with data protection principles those principles 'might well be pitched at a similar level to Cavoukian's legally untethered conception of PbD'.

[17] Cavoukian and Prosch. Dr Cavoukian was the incumbent Information and Privacy Commissioner of Ontario, Canada. The PbD approach she advocated has influenced data protection in the US and is directly referenced in the FTC publications referred to below.

[18] US Govt. Information Infrastructure Task Force (IITF) Privacy Working Group, *Privacy and the National Information Infrastructure: Principles for Providing and Using Personal Information* (6 June 1995) at para 2–4.

[19] Ibid at para 7–8. The report asserts further that appropriateness should be determined based on 'current or planned' activity, and that despite decreasing storage costs it is inappropriate to collect and retain information that is not needed if it may have a 'future unanticipated value'.

In April 2010 the National Institute of Standards and Technology within the US Department of Commerce published special guidelines on protecting the confidentially of 'personally identifiable information' (PII).[20] Although the report does not explicitly refer to PbD, it does reference the principles of the APEC Privacy Framework,[21] which includes, alongside notice and choice,[22] the following principles:

> *'Preventing Harm—Recognizing the interests of the individual to legitimate expectations of privacy, personal information protection should be designed to prevent the misuse of such information. Further, acknowledging the risk that harm may result from such misuse of personal information, specific obligations should take account of such risk, and remedial measures should be proportionate to the likelihood and severity of the harm threatened by the collection, use and transfer of personal information.*
>
> *...*
>
> *Collection Limitation—The collection of personal information should be limited to information that is relevant to the purposes of collection and any such information should be obtained by lawful and fair means, and where appropriate, with notice to, or consent of, the individual concerned.'*[23]

IV THE FTC PRIVACY FRAMEWORK

By December 2010 the FTC had endorsed PbD along with simplified consumer choice and transparency in disclosure notices as best practice approaches in its draft framework for

---

[20] National Institute of Standards and Technology (NIST) and US Department of Commerce, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)* (NIST Special Publications 800-122, April 2010). Also see National Institute of Standards and Technology (NIST) and US Department of Commerce, *Security and Privacy Controls for Federal Information Systems and Organizations* (NIST Special Publication rev 4, 1 April 2015).

[21] APEC, *APEC Privacy Framework* (APEC#205-SO-012, 2005).

[22] The Framework also includes use limitation, security, data integrity, access and correction, and accountability principles.

[23] National Institute of Standards and Technology (NIST) and US Department of Commerce, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)* at D-3. The 'collection limitation' principle mirrors the 'data minimization and retention' principle that is articulated in the FEA-SPP (first published in 2004) in relation to federal agency data handling:
'Data Minimization & Retention
Only collecting PII that is *directly relevant and necessary to accomplish the specified purpose(s)*. Only retaining PII for as long as is necessary to fulfil the specified purpose(s) and in accordance with the National Archives and Records Administration (NARA) approved record retention schedule' (own emphasis).
See National Institute of Standards and Technology (NIST) and others, *Federal Enterprise Architecture Security and Privacy Profile (FEA-SPP) v 3.0* (September 2010).

commercial use of the personal information of consumers.[24] The final FTC privacy framework and accompanying report was published in 2012 after extensive stakeholder engagement indicated broad industry support for a PbD approach.[25]

The FTC has issued subsequent reports in which it advocates a PbD approach in relation to privacy disclosures,[26] mobile applications directed at children,[27] mobile shopping apps,[28] mobile payments,[29] and security.[30] It has also indirectly referenced a PbD approach in regulatory complaints against 'unfair design'[31] and regulatory settlement consent orders requiring the redesign of systems.[32] Although PbD is not explicately referenced in the regulatory guidance issued in relation to health apps,[33] notice to the customers of financial

[24] Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for businesses and policymakers* (March 2012). Transparency and choice are equivalent to notice and consent.
[25] Ibid at 22.
[26] Federal Trade Commission, *Mobile Privacy Disclosures Building Trust Through Transparency* (February 2013). The report emphasises that disclosure is only *one* aspect of a PbD approach.
[27] Federal Trade Commission, *Mobile Apps for Kids: Current Privacy Disclosures are Disappointing* (February 2012), and Federal Trade Commission, *Mobile Apps for Kids: Disclosures Still Not Making the Grade* (December 2012) at 21. The reports contain recommendations for developers, but also emphasise the need for transparency by ad networks and the need for app platforms to enforce privacy standards and develop standardised privacy icons.
[28] Federal Trade Commission, *What's the Deal? An FTC Study on Mobile Shopping Apps* (August 2014).
[29] Federal Trade Commission, *Paper, Plastic ... or Mobile? An FTC Workshop on Mobile Payments* (March 2013) at 69–70.
[30] Federal Trade Commission, *Start with Security: A Guide for Business* (June 2015) Also see Federal Trade Commission, *Mobile Security Updates: Understanding the Issues* (February 2018) which identified the highly variable approach to security updates as problematic, and addresses the complex interactions between OS, device manufactures, and mobile network operators necessary to improve mobile security.
[31] See *Federal Trade Commission v Frostwire LLC and Angel Leon* Case No 111-cv-23643 (SD Fla Oct 12, 2011) (injunction). The FTC was proceeding in this matter not on the basis of a statutory duty to implement 'privacy by design' but on the basis of misleading statements that the FrostWire Android mobile file sharing application and the desktop application allowed users to decide which files they shared publicly (when this was not the case).
[32] See *In the matter of Google Inc.* FTC Dkt No C-4336 (Oct 13, 2011) (consent order), *In the Matter of Facebook Inc* FTC Dkt No C-4365 (Jul 27, 2012) (original consent order) and (Apr 28, 2020) (modified consent order) ( ) and the criticism of Rubinstein and Good at 1407 that the settlements contain only a vague requirement for 'the design and implementation of reasonable controls and procedures to address the risks identified through the privacy risk assessment'.
[33] E.g. US Department of Health and Human Services, 'Health App Use Scenarios & HIPAA' (February 2016) <https://hipaaqsportal.hhs.gov/community-library/accounts/92/925889/Public/OCR-health-app-developer-scenarios-2-2016.pdf> accessed 22 February 2020. Also see Federal Trade Commission, 'Mobile health app developers: FTC best practices' (4 April 2016) <https://www.ftc.gov/tips-advice/business-center/guidance/mobile-health-app-developers-ftc-best-practices> accessed 2 March 2020.

institutions[34] and short form notice for mobile devices,[35] the issues covered by these guidance documents are central to a PbD approach.

(a) General Principles

The FTC summarised its recommendations as follows:

- 'PbD: Build in privacy at every stage of product development;
- Simplified Choice for Businesses and Consumers: Give consumers the ability to make decisions about their data at a relevant time and context, including through a Do Not Track mechanism, while reducing the burden on businesses of providing unnecessary choices; and
- Greater Transparency: Make information collection and use practices transparent.'[36]

The draft framework had outlined a call for companies to 'promote consumer privacy throughout their organizations and at every stage of the development of their products and services'.[37] *The final FTC privacy framework provides:*

'A. The Substantive Principles

Final Principle: Companies should incorporate substantive privacy protections into their practices, such as data security, reasonable collection limits, sound retention and disposal practices, and data accuracy.

B. Procedural Protections to Implement the Substantive Principles

Final Principle: Companies should maintain comprehensive data management procedures throughout the life cycle of their products and services.'[38]

---

[34] Board of Governors of the Federal Reserve System and others, 'Final Model Privacy Notice Form' (17 November 2009) <https://www.sec.gov/news/press/2009/2009-248.htm> accessed 18 February 2020, last amended in 2018.

[35] National Telecommunications and Information Administration (NTIA) US Department of Commerce, *Short Form Notice Code of Conduct to Promote Transparency In Mobile App Practices* (2013 July 25).

[36] Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for businesses and policymakers* at i. The FTC worked closely with the US Department of Commerce which published its own green paper in 2010, followed by a white paper in 2012 calling for a federal consumer privacy statute. The green paper only refers to industry comments supporting PbD in footnotes, while the white paper does not refer to PbD at all. See US Department of Commerce (Internet Policy Task Force), *Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework* (16 December 2010) and US White House Office, *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy* (February 2012).

[37] Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for businesses and policymakers*.

[38] Ibid at i.

It is clear that the report does not alter the intention to promote PbD as an approach to be applied throughout an organisation, and at every stage of product and service development. Rather, the change in wording was intended to make it explicit that PbD is based on, inter alia, the principle that there should be limits upon collection and retention of data.[39]

All three of these principles – PbD, simplified consumer choice and transparency – apply to mobile companies.[40] The report specifically calls for the limitation of collection of data necessary for a requested service or transaction.[41] It also calls for co-operation by all stakeholders within the ecosystem to deliver on privacy: 'carriers, handset manufacturers, operating system providers, app developers, and advertisers … should work together to provide privacy disclosures and ensure that they are understandable, accessible on a small screen, and standardised as to format and terminology for customer's to be able to understand and compare privacy practices'.[42]

(b) Exemption for Small Entities

The FTC Privacy Framework recognises that systematic industry application of the concept of PbD is required,[43] but regulatory requirements must be scaled to the nature and extent of data processing operations.[44] A company that collects small amounts of non-sensitive personal data cannot be required to adopt the same privacy measures as a company collecting vast amounts of data, or processing sensitive data. The final framework applies as follows:

> *'The framework applies to all commercial entities that collect or use consumer data that can be reasonably linked to a specific consumer, computer, or other device, unless the entity collects only nonsensitive data from fewer than 5,000 consumers per year and does not share the data with third parties.'*[45]

---

[39] Ibid at 22–23. Calls for the final framework to explicitly reference all eight principles outlined in the OECD Privacy Guidelines were not followed, with the FTC taking the view that implicitly all eight principles are already covered in the framework. The GDPR 'right to be forgotten' is partially covered by the FTC recommendations that data be deleted when it is no longer needed, and that users have access to data and can request that it be suppressed or deleted in 'appropriate' circumstances.
[40] Ibid at 33.
[41] Ibid at 33.
[42] Ibid at 62.
[43] Ibid at 22.
[44] Ibid at v.
[45] Ibid at 15–16.

The terms 'commercial entities', 'consumer' and 'non-sensitive data'[46] are not defined.

(c) Not an Enforceable Legislative Requirement

Importantly, however, while the FTC regards PbD as an approach as being 'consistent' with FIPPs, it recognises that its recommendations cannot be enforced insofar as they go beyond the legal requirements in existing legislation and it reiterates calls for the enactment of a 'baseline' federal privacy law outlining general principles for the private use of personal information.[47] At present, although the framework does not conflict with the provisions of sector-specific legislation insofar as it exceeds legislative requirements, it is purely a recommendation with no binding force, and is not intended to 'serve as a template' for binding regulatory guidelines and enforcement actions.[48]

For example, the FTC suggests that

> *'it may be appropriate for financial institutions covered by GLBA to incorporate elements of PbD, such as collection limitations, or to improve transparency by providing reasonable access to consumer data in a manner that does not conflict with their statutory obligations'*.[49]

This example is a good illustration of the stark contrast between the emphasis on notice and consent under FIPPS in the US, and the inclusion of the principle of collection limitation (data minimisation) as a condition of lawful processing in GDPR and POPIA.

---

[46] Ibid at 15 and 58–59. The report provides only the following examples of 'sensitive' data, on which there is wide industry consensus, but which cannot be viewed as a closed list: a Social Security number, financial, health, children's, or precise geolocation information. In Federal Trade Commission, *Mobile Security Updates: Understanding the Issues* a much broader definition of 'sensitive personally identifiable information' was adopted, as including 'an individual's Social Security number alone; or an individual's name or address or phone number in combination with one or more of the following: date of birth, Social Security number, driver's license number or other state identification number, or a foreign country equivalent, passport number, financial account number, credit card number, or debit card number.' Further 'sensitive health information' was defined as including 'medical records and other individually identifiable health information relating to the past, present, or future physical or mental health or conditions of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual'.

[47] Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for businesses and policymakers* at i.

[48] Ibid at iii.

[49] Ibid at 16.

The Gramm-Leach-Bliley Act (1999) (GLBA)[50] requires disclosure of data collection, not the minimisation of data collection. Financial institutions governed by the GLBA privacy rule must notify consumers of their information-sharing practices and the right to opt out. A model privacy form has been approved by federal agencies, and use of this form constitutes compliance with the legislative disclosure requirement.[51] In addition, the GLBA safeguards rule[52] requires financial institutions to safeguard customers' personal information[53] through a comprehensive written information security program,[54] and to ensure that their affiliates and service providers[55] comply with those measures.[56]

These are important protections, and they have been applied to mobile application developers.[57] For example, users of PayPal's Venmo app viewed a screen

---

[50] Gramm-Leach-Bliley Act of 1999, Pub.L. No. 106–102, 113 Stat. 1338 (GLBA).

[51] Board of Governors of the Federal Reserve System and others. The form was developed pursuant to amendments to the GLBA introduced in 2006 by the Financial Services Regulatory Relief Act, Pub Law 109–351, 120 Stat. 1966–2010, to require a succinct, comprehensible and readable form that would make it easy for consumers to compare the privacy practices of financial institutions.

[52] Standards for Safeguarding Customer Information, 16 C.F.R. § 314. The Safeguards rule was developed by the FTC pursuant to the GLBA s 501(b).

[53] Ibid §314.2(b). '*Customer information* means any record containing nonpublic personal information as defined in 16 CFR 313.3(n), about a customer of a financial institution, whether in paper, electronic, or other form, that is handled or maintained by or on behalf of you or your affiliates.'

[54]Ibid §314.3. 'Standards for safeguarding customer information.

(a) *Information security program.* You shall develop, implement, and maintain a comprehensive information security program that is written in one or more readily accessible parts and contains administrative, technical, and physical safeguards that are appropriate to your size and complexity, the nature and scope of your activities, and the sensitivity of any customer information at issue. Such safeguards shall include the elements set forth in §314.4 and shall be reasonably designed to achieve the objectives of this part, as set forth in paragraph (b) of this section.

(b) *Objectives.* The objectives of section 501(b) of the Act, and of this part, are to:
  (1) Insure the security and confidentiality of customer information;
  (2) Protect against any anticipated threats or hazards to the security or integrity of such information; and
  (3) Protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer.'

[55] Ibid §314.2(d). '*Service provider* means any person or entity that receives, maintains, processes, or otherwise is permitted access to customer information through its provision of services directly to a financial institution that is subject to this part.'

[56] Ibid §314.4. Inter alia, financial services institutions must:

'(d) Oversee service providers, by:

(1) Taking reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards for the customer information at issue; and

(2) Requiring your service providers by contract to implement and maintain such safeguards.'

[57] *In the Matter of PayPal Inc.* FTC Dkt No C-4651 (May 24, 2018) (consent order), concerned a consent order against PayPal for deceptive communications about its Venmo app. One aspect of the complaint related to the representation that 'Venmo uses bank-grade security systems and data encryption to protect your financial information.' In fact Venmo had inadequate safeguards for the security, confidentiality, and integrity of consumer information. E.g. failure to notify users about account changes (such as changes of password or e-mail address, and the addition of a second email or device) had in some instances permitted fraudster's to take over user's Venmo accounts and withdraw the funds without the user's knowledge.

containing a notice printed in grey text on a light grey background. This did not comply with the Privacy Regulation and Regulation P as it was not 'clear and conspicuous' nor was it 'designed to call attention to the nature and significance of the information in the notice'.[58] Use of a different size and colour of font to stand out from the background, and some reference to third party sharing of data (and other practices the user might not reasonably expect to find in the privacy policy) should have been outlined in a short form notice on the initial screen.

The screen informed the user that '[b]y signing up, you are agreeing to Venmo's User Agreement and Privacy Policy'. Below that was a link to the Privacy Policy and the Terms and Conditions. This did not meet the requirement that the customer must reasonably be expected to have received actual notice before accessing the product or service. An opt-in consent mechanism which could record the user's consent should have been included.

Lastly, the privacy policy itself contained inadequate disclosures about PayPal's sharing of personal information with third parties. The policy represented that PayPal would share a user's personal information only 'with the user's "social web if [the user's] Venmo account transactions are designated as 'public' or friends-only payments …"', which was incorrect.[59] By default, all the names of payer and recipient and any message by the payer were displayed on the user's Venmo social news feed, and the five most recent payments were viewable on the user's public profile by any person viewing the Venmo web page.[60] The privacy settings were not user-friendly as, to achieve privacy, a user had to change to separate settings and this was not clearly explained to users. Thus a user who changed the 'audience' setting from 'public' to 'participants only' but failed also to change the 'transactions' setting from 'everyone' to 'only me', would still find that some transaction could be publicly displayed.[61]

This was contrary to user's reasonable expectations, and did not comply with the GLBA as a privacy notice is required to specify the categories of 'non-public personal information' collected or disclosed by the 'financial institution' and the categories of third

[58] Ibid (Complaint, para 38).
[59] Ibid.
[60] Ibid (complaint, para 17–31).
[61] Ibid.

parties to whom disclosures are made, as well as the security and confidentiality of the information.[62] The consent order required PayPal to correct these violations, inter alia by

> *'provid[ing] clear and conspicuous disclosures to users related to how any payment and social networking service shares transaction information with other users and how a consumer can limit the visibility or sharing of transaction information through privacy settings'*.[63]

However, if such institutions were to adopt a PbD approach, they would by default collect only such information as was necessary for a clearly specified purpose of processing, allowing customers a choice to express affirmative consent (opt-in) to additional collection, at a granular level that permits real choice about whether to allow collection for some purposes (which could be conditional where they are truly necessary for a core function of the service) and not to allow collection for other purposes. Incorporating the principles of openness (through clear comprehensive notice), purpose specification, and minimality and a requirement for voluntary, specific and informed consent would mean that default settings and system design would be optimised for privacy, rather than placing the onus on customers to read privacy disclosures and opt out of collection.

(d) Lack of Clarity on Data Minimisation

The FTC Privacy Framework illustrates the difficulty of reconciling the principle of 'data minimisation' that is central to the PbD approach, and particularly the requirement that data should be protected by default,[64] with the flexibility demanded by industry, particularly with regard to the use of data analytics for product enhancement and development, and the use of targeted advertising.

The principle of collection limitation as articulated in the OECD Guidelines is synonymous with a degree of data minimisation, in that only personal information that is

---

[62] GLBA 16 C.F.R. § 313.6; 12 C.F.R. § 1016.6.
[63] *In the Matter of PayPal Inc.* (Agreement containing Consent Order, 27 February 2018).
[64] Cavoukian, 'Privacy by Design The 7 Foundational Principles Implementation and Mapping of Fair Information Practices'. Cavoukian 'maps' the principle of data minimisation to the principle that privacy should be a default setting. Her analysis obfuscates an important issue by referring to both collection limitation and data minimisation without clarifying the difference in origin or meaning. Collection limitation is then defined as imposing 'fair and lawful' limits on collection to what is 'necessary' for 'specified purposes', whereas data minimisation is referred to as keeping the collection of personal information to a 'strict minimum'. It is submitted the principles should be viewed as synonymous- and limited by 'reasonableness'/'fairness.'

directly relevant to or necessary for the specified purposes should be collected and processed, and such personal information must be deleted or de-identified as soon as possible.[65] This permits personal information to be collected for purposes that go beyond what is strictly necessary for the service or function being performed, but is limited by what is reasonable, by the specification of a clear purpose in a disclosure notice and, where necessary, voluntary, specific and informed user consent.

However, as outlined in chapter 1 of this dissertation, even at this level, the principle of data minimisation is at odds with the ethos of big data analytics, which is that data may yield future, unanticipated insights and drive innovation. This perspective was conveyed strongly in stakeholder comments on the FTC Privacy Framework.[66] It is reiterated in a 2018 global survey of app developers.[67] The FTC has maintained a stance that there must be a 'reasonable collection limitation'. The FTC's reports make it clear that what is reasonable is limited by what is necessary in the context of the transaction.[68] The FTC has proposed that notice and consent are not required for collection that is consistent with the context of the transaction, but that for any collection 'inconsistent with these contexts, companies should make appropriate disclosures to consumers at a relevant time and in a prominent manner – outside of a privacy policy or other legal document'.[69] By failing to clarify what would constitute an 'appropriate' disclosure, the recommendation addresses neither the concern of industry that it is difficult to specify purposes clearly,[70] nor the FTC's concern that 'vague'

---

[65] This was the approach taken in the preliminary staff report. See Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for businesses and policymakers* at 26. For an example of its practical implementation see the internal guidelines for data handling issued by the Department of Homeland Security (DHS) Privacy Office, *Handbook for Safeguarding Sensitive PII, Privacy Policy Directive 047-01-007, Revision 3* (2017) which reference eight principles: Transparency, Individual Participation, Purpose Specification, Data Minimization, Use Limitation, Data Quality and Integrity, Security, and Accountability (and Auditing). Data minimisation is described in that report as follows: 'DHS should only collect PII that is directly relevant and necessary to accomplish the specified purpose(s) and only retain PII for as long as is necessary to fulfil the specified purpose(s)'.

[66] Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for businesses and policymakers* at 26.

[67] App Developers Alliance, *Developers See the Need for Best Practices in Data Sharing & Security, Spring 2018 Data Survey of 100+ Developers and Appreneurs* (2018) at 2. 89% believe data sharing is indispensable to building a successful product or company.

[68] Also see Michelle Finneran Dennedy, Jonathan Fox and Thomas R. Finneran, *The Privacy Engineer's Manifesto: Getting from Policy to Code to QA to Value* (Apress Open 2014) at 44–45 proposing a simple model for compliance with the OECD's collection limitation principle: what is needed, not what is wanted.

[69] Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for businesses and policymakers* at 27.

[70] Ibid at 26.

promises would allow data collectors to do virtually anything with the data.[71] For example, it would be unclear if the developer of a direction-finder app has complied with its obligations if the user has granted permission for the app to access location services,[72] and the privacy policy states that personal information (which could be specified but still unclear to the user, for example, 'aggregated location data')[73] may be used to 'personalise the service we offer you'[74] and for 'product improvement and development'.[75]

The FTC's report on mobile payments applies the same 'context-based' collection limitation recommending that

> *'companies should consider giving consumers the choice to restrict disclosure of information that is not necessary for completing a payment transaction, or that use of payment data for other purposes or by third parties should not be pre-selected as default options'*.[76]

In accordance with a PbD approach, collection is limited to what is necessary, and explicit 'opt-in' consent is required for the collection of data that is not necessary in the context of the transaction or for the use of data for any purposes outside the context of the transaction. One advantage of this approach is that consumers are notified only about collection which they would not already reasonably expect. This may be more effective than overly extensive disclosures which can actually impede a consumer's ability to make informed choices,[77] leading to 'click fatigue'. However a key impediment to the implementation of Pb(re)D in the mobile apps ecosystem, where there are complex multi-party and multi-layer

---

[71] Ibid at 27.
[72] As explained in chapter 2, permissions are determined by the OS. A user seeing a run time permission request may assume the purpose of collection is related to the current use of the app (e.g. searching for directions to an address from one's current location). The permission request would not alert the user to additional purposes for collection outlined in the privacy policy (if there is one), nor would it alert the user to the possibility of the app running in the background and transmitting continuous location data even when the app is not in use.
[73] As explained in chapter 2, no standards exist for 'aggregation', 'anonymisation' and 'pseudonymisation' techniques, and the user thus does not know how the app developer will handle its data.
[74] Such a disclosure would evidently cover innocuous uses of data, such as permitting the app to personalise 'greetings' and in-app notifications. Arguably however it would also cover the delivery of targeted advertising.
[75] The analysis of app data, such as app 'crash' reports, is essential to ensure that the product is functioning as intended, and to permit app developers to address problems and improve user experience. Arguably, however, it would also cover use of location data to improve traffic pattern algorithms, or even to develop new products altogether.
[76] Federal Trade Commission, *Paper, Plastic ... or Mobile? An FTC Workshop on Mobile Payments* at 70–71.
[77] Federal Trade Commission, *Mobile Security Updates: Understanding the Issues* at 73.

data processing operation, is the lack of clarity on which party is accountable to ensure that notice is given and the data minimisation principle is implemented.

(e) An Accountability Gap?

A key insight from Pb(re)D is that the effective implementation of Pb(re)D in the mobile apps ecosystem requires that all role-players: developers, device manufactures, OS platforms, carriers and app stores, take responsibility for ensuring that mobile apps do not pose an unreasonable risk to the privacy and security of app user's personal information.

In short, privacy must be implemented throughout the organisation *and* the ecosystem if it is to be effectively protected. But as chapter 2 illustrated, the mobile apps ecosystem is complex, involving multiple parties in the 'downstream' processing of data collected by the app, and multiple 'upstream' parties who develop the technologies and platforms upon which mobile apps are built and marketed.

A recent comprehensive literature review of technical studies on PbD revealed that none of those studies addressed how to approach Pb(re)D in relation to third-party processing.[78] The FTC has emphasised that notice and consent are not a substitute for security.[79] What the FTC does not address is the extent to which an operator or business is responsible for ensuring that it does not disclose personal information to third parties who will not adopt adequate security measures, and the extent to which upstream suppliers of technologies and platforms are responsible for the security vulnerabilities in their products. While developers cannot guarantee that no security breach will occur, by adopting a PbD approach, they should proactively assess possible risks and take all reasonable steps to secure personal information, rather than relying on a contractual limitation of liability.[80] However,

---

[78] Christian Kurtz and Martin Semmann, 'Privacy by Design to Comply with GDPR: A Review on Third-Party Data Processors' (Twenty-fourth Americas Conference on Information Systems, New Orleans, 2018) at 7concluding that the lack of lack of 'feasible, accepted designs and implementations for dealing with third parties is a major research gap'.

[79] Federal Trade Commission, *Mobile Security Updates: Understanding the Issues* at 1.

[80] John Daley, 'Insecure Software is Eating the World: Promoting Cybersecurity in an Age of Ubiquitous Software-embedded Systems' (2017) 19 *Stan Tech L Rev* 533–546 at 536–537 argues that developers have been permitted to blame cybercriminals and user apathy 'rather than acknowledging the obvious risks created by their own lack of adequate testing and flawed software design.'

market forces alone may be insufficient to achieve such an outcome[81] unless liability to meet minimum security standards is imposed by law.[82]

V CALIFORNIA ATTORNEY GENERAL GUIDELINES

The Attorney General of California has issued general guidelines to mobile application developers,[83] which followed a preliminary 'factsheet'[84] and a ground-breaking agreement with app platforms Apple and Google. This agrement led to the introduction of a compulsory privacy policy requirement for listing in the app stores from 2012.[85] Similar guidelines to mobile application developers have been issued by data protection and privacy commissioners

[81] See for example Robert W Hahn and Anne Layne-Farrar, 'The Law and Economics of Software Security' (2006) 30 *Harv JL & Pub Pol'y* 283–354 and Ginger Zhe Jin and Andrew Stivers, 'Protecting Consumers in Privacy and Data Security: A Perspective of Information Economics' [2017] <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3006172> accessed 15 May 2020. Both are cited by the FTC in its report on security in relation to the high degree of 'information asymmetry' between users and developers. Users do not understand how data will be used and secured, and must rely on representations by developers which they cannot verify. As a consequence users may undervalue security.

[82] Daley at 537–538. Daley criticises a purely contractual model of liability based on caveat emptor (buyer beware) as inappropriate to software systems where 'information asymmetry' is high. However, as he explains, there remains scholarly disagreement about the extent of developer liability for security vulnerabilities and upon whether developer liability should lie in contract, product liability, strict liability, no-fault liability, or negligence.

[83] State of California Office of the Attorney General, *Privacy on the Go: Recommendations for the Mobile Ecosystem* (2013) at 4. While the recommendations are primarily addressed to app developers they expressly call on all role-players to be accountable for data privacy and 'to consider privacy at the outset of the design process.'

[84] State of California Office of the Attorney General, *Mobile Applications and Mobile Privacy Fact Sheet* (2012).

[85] State of California Office of the Attorney General, *Agreement to Strengthen Privacy Protections for Users of Mobile Applications* (22 February 2012).

in Australia,[86] Hong Kong,[87] Canada,[88] and the United Kingdom,[89] and the recommendations are consistent with the opinions of the Article 29 Working Group in Europe.[90]

(a) General Principles

The report does not expressly reference PbD but does indicate that the guidelines 'are intended to encourage all players in the mobile marketplace to consider privacy implications *at the outset* of the design process'.[91]

Transparency and a user-centric approach are anchored by four recommendations:

---

[86] Office of the Australian Information Commissioner, *Mobile privacy: A better practice guide for mobile app developers* (2014). The guidance advocates a PbD approach, but does not suggest that this is a legal obligation, only that following such an approach 'will help you make your apps more privacy-friendly.' The guidance must be considered together with Australia's Privacy Act 1988 (Cth) and the 10 Australian Privacy Principles it contains.

[87] Office of the Privacy Commissioner for Personal Data Hong Kong, *Personal data privacy protection: what mobile apps developers and their clients should know* (2012). The guidance must be considered together with Personal Data (Privacy) Ordinance, Laws of Hong Kong (Cap 486) (PDPO).

[88] Office of the Privacy Commissioner of Canada (OPC), *Seizing Opportunity: Good Privacy Practices for Developing Mobile Apps* (2012) and OPC, 'Ten tips for communicating your app's privacy practices to your app's users' (September 2014) <https://www.priv.gc.ca/en/privacy-topics/technology/mobile-and-digital-devices/mobile-apps/02_05_d_61_tips/> accessed 18 February 2020. The guidance must be considered together with Canada's Personal Information Protection and Electronic Documents Act S.C. 2000, c.5, and the 10 fair information principles. A number of other OPC guidelines are also relevant to app developers generally: OPC, *Processing Personal Data Across Borders Guidelines* (2009), OPC, *Reaching for the Cloud(s): Privacy Issues related to Cloud Computing* (2010), OPC, *Report on the 2010 Office of the Privacy Commissioner of Canada's Consultations on Online Tracking, Profiling and Targeting, and Cloud Computing* (2011), OPC and others, *Securing Personal Information: A Self-Assessment Tool for Organizations* (2012) ; OPC and others, *Getting Accountability Right with a Privacy Management Program* (2012); OPC, *Cloud Computing For Small- And Medium-Sized Enterprises: Privacy Responsibilities and Considerations* (2012) and OPC, 'Guidelines for Obtaining Meaningful Consent' (May 2018) <https://www.priv.gc.ca/en/privacy-topics/collecting-personal-information/consent/gl_omc_201805/> accessed 18 February 2020.

[89] Information Commissioner's Office (UK) (ICO), *Privacy in Mobile Apps: Guidance for App Developers* (2013). The guidance pertains to the Data Protection Act 1984 (c. 35) and has not been updated to reflect GDPR and the Data Protection Act 2018 (c.12). Also see ICO, *The Right to be Informed* (2018), which contains detailed guidance on how to use layered privacy policies and just in time notices in a mobile app.

[90] Article 29 Data Protection Working Party, *Opinion 02/2013 on apps on smart devices* (WP 202, 27 February 2013). The opinion must be read together with the Article 29 working party's guidance in related areas, chiefly Article 29 Data Protection Working Party, *Opinion 4/2007 on the concept of personal data* (WP 136) ; Article 29 Data Protection Working Party, *Opinion 1/2010 on the concepts of "controller" and "processor"* (WP 169, 16 February 2010) ; Article 29 Data Protection Working Party, *Opinion 13/2011 on Geolocation services on smart mobile devices* (WP185, 16 May 2011) ; Article 29 Data Protection Working Party, *Guidelines on Consent under Regulation 2016/679* (WP 259, 28 November 2017) ; Article 29 Data Protection Working Party, *Opinion 2/2010 on online behavioural advertising* (WP 171, 22 June 2010) ; Article 29 Data Protection Working Party, *Opinion 3/2010 on the Principle of Accountability* (WP173, 13 July 2010).

[91] State of California Office of the Attorney General, *Privacy on the Go: Recommendations for the Mobile Ecosystem* at 4.

1. Make a general privacy policy that is comprehensive but easy to understand[92] available before download (that is, accessible in the app store),[93] and via links on the app's home screen and the app website.[94]

2. Include a short privacy statement[95] (in the app store and in the app) describing collection of 'sensitive' information, or any other use of data that could be 'unexpected' because it is not necessary for the app's basic functionality.[96]

3. Use special notices delivered 'just in time' in the context of a particular use of the app to alert users to collection of sensitive information, or information not needed for the basic functionality of the app.[97]

4. Provide user privacy settings that are accessible and easy to change.[98]

---

[92] Ibid. The report defines 'general privacy policy' as 'a comprehensive statement of a company's or organization's policies and practices related to an application, covering the accessing, collecting, using, disclosing, sharing, and otherwise handling of personally identifiable data.' The report does not address whether as a matter of best practice a privacy policy should be produced by apps which do not collect personal information (but may collect other data) or whether the policy should address what use is made of anonymised (de-identified) data.

[93] In the 2012 agreement with app marketplaces, app developers were to be given an option to provide a hyperlink to their privacy policy, or a text summary of the app's privacy practices, which would be made accessible to users in the app store. See State of California Office of the Attorney General, *Agreement to Strengthen Privacy Protections for Users of Mobile Applications*.

[94] Although the report recommends the privacy policy be hosted on the app's website to facilitate updates, it does not address when and how updates should be communicated to user (or whether users are responsible for periodically checking the privacy policy).

[95] A 'short privacy statement' is defined as 'a privacy policy designed to be read on a mobile device, highlighting data practices that involve sensitive information or are likely to be unexpected because they involve data not required for an app's basic functionality.' State of California Office of the Attorney General, *Privacy on the Go: Recommendations for the Mobile Ecosystem* at 6.

[96] Clearly all collection of personal information to facilitate in-app advertising in free apps is a use that would be unexpected on this definition and must be expressly disclosed, even if the data is shared in an anonymous, pseudonymous or aggregated format.

[97] State of California Office of the Attorney General, *Privacy on the Go: Recommendations for the Mobile Ecosystem* at 6. A 'special notice' is defined as 'a timely, contextual notice that alerts users to a data practice that is likely to be unexpected because it involves sensitive information or data not required for an app's basic functionality.' E.g. when a runtime permission to access location is requested. Although not expressly addressed in the report, the permission request should include a short explanation of why the data is collected. Thus if location is collected both for app functionality and for unexpected uses, the special notice should highlight the unexpected use. A user can then refer to the privacy policy for further information.

[98] Ibid. 'Privacy controls are settings available within an app or an operating system that allow users to make or revise choices offered in the general privacy policy about the collection of their personally identifiable data.'

Although the terms 'personally identifiable data'[99] and 'sensitive personally identifiable data'[100] are defined, their use is consistent neither with California legislation, nor with the wider definition adopted in reports by the FTC.[101]

(b) No Exemption for Small Entities

Although the report acknowledges that many developers are small entities or individuals,[102] no reference is made to exemptions.

(c) Not an Enforceable Legislative Requirement

The guidance acknowledges that in certain respects it exceeds legislative requirements,[103] without providing further clarification.

(d) Lack of Clarity on Data Minimisation

The report encourages 'surprise minimisation', that is, to 'minimize surprises to users from unexpected privacy practices'.[104] However, like the FTC Privacy Framework, it fails to provide an explanation of how to reconcile the inherent tension between data minimisation and the requirements of data analytics and targeted advertising.

Early on, 'surprise minimisation' is explained as requiring app developers to 'avoid collecting personally identifiable data from users that are not needed for an app's basic

---

[99] Ibid. The term 'personally identifiable data' is defined as 'any data linked to a person or persistently linked to a mobile device: data that can identify a person via personal information or a device via a unique identifier. Included are user-entered data, as well as automatically collected data.'

[100] Ibid. The term 'sensitive information' is defined as 'personally identifiable data about which users are likely to be concerned, such as precise geo-location; financial and medical information; passwords; stored information such as contacts, photos, and videos; and children's information.'

[101] Federal Trade Commission, *Mobile Security Updates: Understanding the Issues*. For example the California AG does not consider whether information *becomes sensitive when combined* with other information. E.g. a person's name when used in combination with their email address. On the other hand the California AG refers to 'stored information' such as contacts, photos and videos as sensitive. While the FTC reports discussed above do not mention these as 'sensitive' the California AG may be impliedly referencing Google's classification of 'dangerous' permissions 'where the app wants data or resources that involve the user's private information, or could potentially affect the user's stored data or the operation of other apps.' Android Developers, 'Permissions Overview' <https://developer.android.com/guide/topics/permissions/overview#dangerous_permissions> accessed 31 August 2019.

[102] State of California Office of the Attorney General, *Privacy on the Go: Recommendations for the Mobile Ecosystem* at 7.

[103] Ibid at 4.

[104] Ibid at 5.

functionality',[105] but later app developers are advised to 'avoid *or minimize* the collection of personally identifiable data for uses not related to your app's basic functionality'[106] (own emphasis). This is combined with the advice to 'use an app-specific or other nonpersistent device identifier rather than a persistent, globally unique identifier'. This could suggest to app developers that collection of data linked to a 'nonpersistent' identifier is not personally identifiable information[107] (which may also imply that no notice of such collection is necessary),[108] even if this data is shared with third party advertisers.[109] Further, this suggests to developers that an app developer complies with the collection limitation principle if users consent to the collection of personal information for purposes that go beyond app functions. By indicating that the 'default settings should be privacy protective'[110] the report complies with the second principle of PbD, but it stops short of requiring 'full functionality' even if a user does not consent to additional data sharing. [111]

(e) An Accountability Gap?

Finally, the California guidelines do not adequately address either the accountability for downstream data processing by third parties such as ad networks, or the accountability of upstream technology and platform providers.

VI SELF-REGULATION IS INSUFFICIENT

The FTC has applauded industry efforts towards developing privacy policy generators, privacy seals, and self-regulatory codes. However, although the FTC has indicated that it will regard

---

[105] Ibid. As such the report is in line with the view that data limitation/data minimisation requires that data is only collected if it is needed for an app function, rather than wanted by the developer or a third party for other purposes.
[106] Ibid at 9.
[107] Ibid at 8 where only a 'unique device identifier' was described as personally identifiable information. If the report intended to exclude semi-persistent identifiers such as an advertising identifier (described in chapter 2) this ignores the extent to which de facto tracking is possible unless identifiers are regularly reset.
[108] Ibid at 9 the report states: 'Give users control over the collection of any personally identifiable data used for purposes other than the app's basic functions.'
[109] Ibid at 12. The report indicates that 'special notice' is probably needed for 'the disclosure to third parties of personally identifiable information for their own use, including use for advertising'. Although the report does not clearly indicate that use of an advertising ID constitutes personal information, this approach should be taken to ensure users cannot be served targeted advertising without their opt-in consent. If personally identifiable information is shared with service providers who do not use it for their own purposes, a special notice is not required (although this should be disclosed in the privacy policy).
[110] Ibid at 9.
[111] Ibid. The report simply states: 'You may want to explain the consequences of not allowing the collection of the data.' Further (at 12) the report recommends 'Avoid take-it-or-leave-it choices, but when an app developer makes use of the app contingent on collection of the data, that choice should be made clear.'

compliance with the NTIA short form code of conduct favourably,[112] none of these codes are endorsed by federal agencies[113] or state law enforcement.[114] This may act as a disincentive to companies, as adopting the code is not a guarantee of legislative compliance, and may expose a company to regulatory action if its stated adoption of the code is inconsistent with its actual privacy practices.

Furthermore, there is now a proliferation of industry voluntary guidelines. These include best practice guidelines issued by the Future of Privacy Forum,[115] the World Wide Web Consortium,[116] the Electronic Frontier Foundation,[117] the CTIA Guidelines on location-based services,[118] the Trust-e Privacy-by-Design guidelines,[119] the Network Advertising Initiative (NAI) Code of Conduct (2020),[120] and the GSMA Mobile Privacy Principles[121] and Privacy Design Guidelines for Mobile Application Development.[122]

Despite industry efforts to provide a tool for consolidating some of these guidelines[123] and developing online privacy policy generators,[124] open source code for mobile

---

[112] Federal Trade Commission, *Mobile Privacy Disclosures Building Trust Through Transparency* at 12.
[113] National Telecommunications and Information Administration (NTIA) US Department of Commerce, expressly records that compliance with the NTIA short form code of conduct is not a guarantee of legislative compliance.
[114] The State of California Office of the Attorney General, *Privacy on the Go: Recommendations for the Mobile Ecosystem* records that its report should not be construed as legal advice or the policy of the state of California.
[115] Future of Privacy Forum and Center for Democracy & Technology, 'Best Practices for Mobile Application Developers' (12 July 2012) <https://fpf.org/wp-content/uploads/Apps-Best-Practices-v-beta.pdf> accessed 28 February 2020.
[116] World Wide Web Consortium (W3C), *Web Application Privacy Best Practices W3C Working Group Note* (3 July 2012).
[117] Electronic Frontier Foundation (EFF), *Mobile User Privacy Bill of Rights* (2012).
[118] CTIA The Wireless Association, *Best Practices and Guidelines for Location Based Services v2* (2010).
[119] TrustArc, *Truste's Privacy-by-Design Guidelines* (2012)
[120] Network Advertising Initiative (NAI), 'The NAI Code of Conduct' (2020) <https://www.networkadvertising.org/code-enforcement/code> accessed 2 March 2020. The NAI published a code of conduct for web-based advertising in 2000. In 2013 it published The Mobile Application Code. Both codes were updated periodically and have now been updated and consolidated in the 2020 code. In addition the NAI has published guidance on use of health data, imprecise location data, viewed content data, cookies, cross-device tracking, and opt-in consent.
[121] GSM Association (GSMA), *Mobile Privacy Principles: Promoting Consumer Privacy in the Mobile Ecosystem* (January 2011). The GMSA (Global System for Mobile Communications, originally Groupe Spécial Mobile) is an association representing cellular network operators.
[122] GSM Association (GSMA), *Privacy Design Guidelines for Mobile Application Development* (February 2012).
[123] International Association of Privacy Professionals (IAPP) Westin Research Centre, 'Comparison of Mobile Applications Guidelines' <https://iapp.org/resources/comparison-of-mobile-application-guidelines/> accessed 2 March 2020. The tool does not consider the guidelines issued by NIST, CTIA, Truste, or GSMA.
[124] E.g. TermsFeed, 'Privacy Policy Generator' <https://www.termsfeed.com/privacy-policy-generator/> accessed 2 March 2020, and Iuebenda.com, 'Iuebenda Privacy Policy Generator' <www.iubenda.com/> accessed 15 May 2020. There are a number of such tools online. These are examples only and each app developer must develop a policy based on their actual data practices.

privacy disclosures[125] and privacy 'seals',[126] complexity remains a problem. Without regulatory oversight through an approved code of conduct, there is little to guide developers or consumers with regard to the trustworthiness and adequacy of such tools and programs.

Moreover, all of the regulatory and industry guides considered in this study were textual restatements of data protection principles or policy. They reiterate that privacy must be 'built into' design but do not provide clarity on what this means.[127] Industry[128] and scholars[129] agree that what is required are interoperable tools, standards and best practice methodologies for the technical implementation of data protection principles in the design of IT systems.[130]

---

[125] Association for Competitive Technology (ACT) The App Association, 'Privacy Dashboard' <https://actonline.org/projects/privacy-dashboard/> accessed 2 March 2020. Also see the online guidance for all apps, children's apps, health apps and finance and e-commerce apps provided by Association for Competitive Technology (ACT) The App Association, 'App Privacy and Transparency' <https://actonline.org/privacy/> accessed 2 March 2020.

[126] E.g. Android, 'Android PlayProtect' <https://www.android.com/play-protect/> , and 'TRUSTe Assurance ' <https://www.trustarc.com/> accessed 16 May 2019.

[127] Rubinstein and Good at 1407.

[128] App Developers Alliance. Also see European Network and Security Agency, *Privacy and Data Protection by Design: From Policy to Engineering* (2014) at 49–50 and European Union Agency For Network and Information Security, *Privacy and data protection in mobile applications: A study on the app development ecosystem and the technical implementation of GDPR* (November 2017) at 62.

[129] Rubinstein and Good at 1408. Also see Harshvardhan J Pandit and others, 'Creating a Vocabulary for Data Privacy' in Hervé Panetto and others (eds), *OTM Consolidated International Conferences: On the Move to Meaningful Internet Systems* (Springer, Rhodes, Greece 21–25 October 2019) at 2.

[130] It is beyond the scope of this dissertation to analyse the technical standards and models for privacy. For the first taxonomy of personal data items and processing purposes see Harshvardhan J. Pandit and Axel Polleres, *Data Privacy Vocabulary v0.1 Draft Community Group Report* (Data Privacy Vocabularies and Controls Community Group, W3C Consortium, 28 November 2019). For related recent and current work see ISO, *Information technology — Online privacy notices and consent* (ISO/IEC FDIS 29184 [ISO/IEC DIS 29184]); National Institute of Standards and Technology (NIST), *Digital Identity Guidelines SP 800-63-3* (2017), Mark Lizar and David Turner, *Consent Receipt Specification v1.1.0.* (Kantara Initiative Recommendation, 20 February 2018), Eve Maler and ForgeRock, *User-Managed Access (UMA) 2.0 Grant for OAuth 2.0 Authorization* (Kantara Initiative Recommendation, 1 July 2018), SPECIAL H2020 projects described in Piero A Bonatti and others, 'Machine Understandable Policies and GDPR Compliance Checking' [2020] *arXiv preprint arXiv:200108930*, United Nations Commission on International Trade Law Fiftieth session, *Report of Working Group IV (Electronic Commerce) on the work of its fifty-fourth session (Vienna, 31 October–4 November 2016)* (2017), Paul Bruton and others, *Classification of Everyday Living Version 1.0.* (OASIS Committee Specification 02, 26 June 2018), OASIS, *Privacy Management Reference Model and Methodology (PMRM) Version 1.0.* (2013), American Institute of Certified Public Accountants (AICPA) and Canadian Institute of Chartered Accountants (CICA) Privacy Task Force, *Privacy Maturity Model* (March 2011), and Mark Lizar and Harshvardhan J Pandit, 'OPN: Open Notice Receipt Schema' (2019) <http://ceur-ws.org/Vol-2451/paper-21.pdf> accessed 24 February 2020. For additional web standards see Lebo Tim, Satya Sahoo and Deborah McGuinness, *PROV-O: The PROV ontology : W3C recommendation 30 April 2013* (W3C Recommendation, 2013); Daniel Garijo and Yolanda Gil, *The P-PLAN Ontology* (12 March 2014); S Villata and R Iannella, *ODRL Information Model 2.2* (W3C Recommendation, 15 February 2018); R Iannella and J (May 2014) McKinney, *vCard Ontology - for describing People and Organizations* (W3C Interest Group Note, 22 May 2014), Schema.org, 'Schema v6.0' <https://schema.org/docs/releases.html> accessed 24 February 2020 and James M. Snell and Evan Prodromou, *Activity Streams 2.0* (W3C Recommendation, 23 May 2017). Also see IEEE, *P7012 - Standard for Machine Readable Personal Privacy Terms* (2017).

The OASIS PbD technical subcommittee produced a draft specification for mapping PbD to software engineering documentation,[131] but the subcommittee was closed in September 2019 and a final specification was never published.[132]

With regard to larger and well-resourced enterprises building custom apps, it may be possible for them to develop their own software development guides,[133] or reference existing standards[134] such as the ISO/IEC 27701,[135] Common Criteria for Information Security Evaluation,[136] FIPS 140-2[137] and Business Process Model and Notation (BPMN)[138] extensions.[139] For small and medium-sized enterprises, less complex approaches must be developed.[140] What a PbD approach emphasises in all cases is that employing any particular PET, such as encryption, is not a complete solution.[141]

---

[131] Ann Cavoukian and others, *Privacy by Design Documentation for Software Engineers Version 1.0.* (OASIS Committee Specification Draft 01, 25 June 2014).

[132] OASIS, 'OASIS Privacy by Design Documentation for Software Engineers (PbD-SE) TC' <https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=pbd-se> accessed 2 March 2020.

[133] E.g. the adoption of PbD by IBM, Sun Microsystems, Hewlett Packard and Microsoft discussed in Rubinstein and Good at 1335 and 1408.

[134] The ISO's Information Technology sub-committee alone has 3236 published standards and 564 standards under development. These include a draft standard on privacy notice and a published standard on privacy impact assessments. See ISO, *Information technology — Online privacy notices and consent* (ISO/IEC FDIS 29184) and ISO, *Information technology — Security techniques — Guidelines for privacy impact assessment* (ISO/IEC DIS 29134, 2017) ; ISO, ''Technical Committees'' <https://www.iso.org/technical-committees.html> accessed 3 March 2020.

[135] ISO, *Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines* (ISO/IEC 27701, 2019).

[136] *Common Criteria for Information Technology Security Evaluation v3.1 rev 5* (CC v31 Release 5 ISO/IEC 15408, 2017).

[137] National Institute of Standards and Technology (NIST) and US Department of Commerce, *Security Requirements for Cryptographic Modules* (FIPS 140-142, 25 May 2001).

[138] Object Management Group (OMG), *Business Process Model and Notation (BPMN) v2.02* (ISO/IEC 19510, January 2014). Version 1.0 of the standard was published in 2007.

[139] For a literature review of technical studies see Karim Zarour and others, 'A Systematic Literature Review on BPMN Extensions' [2019] *Business Process Management Journal*. For recent efforts to detect conflicts between security (collecting authentication credentials) and data minimization using SEC-BPMN2 extension and ISO/IEC 15408, see Qusai Ramadan and others, 'A Semi-automated BPMN-based Framework for Detecting Conflicts between Security, Data-minimization and Fairness Requirements' [2020] *Software and Systems Modeling* 1–37.

[140] See e.g. the definition of an app use case and simple context and component diagrams constructed using Unified Modelling Language (UML) to map the privacy components of a 'runner's app' being developed by a start-up enterprise in chapter 8 of Finneran Dennedy, Fox and Finneran, or even a simple checklist as recommended by and the use of a simple checklist or matrix recommended in State of California Office of the Attorney General, *Privacy on the Go: Recommendations for the Mobile Ecosystem* at 8–9. Also see *Software engineering — Lifecycle profiles for Very Small Entities (VSEs)* (ISO/IEC 29110-2-1:2015).

[141] Finneran Dennedy, Fox and Finneran at 153: 'Even if the design is full of PETs, privacy will not be fully protected without well-written policies, standards, procedures, guidelines, and a notice presented in a readable form, among other things. PETs are enablers, but they are not substitutes for privacy engineering. PETs can be just one of many design components but alone are not a privacy solution.'

Arguably, the self-regulatory approach has failed because the absence of a regulatory imperative to implement privacy by design and weak consumer demand for privacy technologies act as a disincentive to developers.[142]

VII REGULATORY ENFORCEMENT ACTIONS AGAINST APP DEVELOPERS

A review of regulatory actions by the FTC shows that there has been progressively more stringent enforcement of COPPA provisions against mobile app developers and other online services. In 2011 the FTC charged app developer W3 Innovations LLC and its owner, Justin Maples, with violating COPPA in relation to the app 'Emily's Girl World' and related apps 'Emily's Dress Up' 'Emily's Dress Up & Shop', and 'Emily's Runway High Fashion'.[143] The apps were available from 2009 in the Apple App Store and based on their subject matter, and promotional statements on the app developer's website, they were clearly targeted at young, elementary school girls. The app 'Emily's Girl World' was downloaded over 30 000 times.

There was no link to a privacy policy. No notice was given of the app's collection, use and disclosure of personal information. At the time, it was not uncommon for mobile apps to have no privacy policy.[144] It was only in 2012, after the FTC charges against Emily's Girl World, and public outrage over other 'industry standard practices',[145] that the California Attorney General announced that CalOPPA required mobile apps to post a 'conspicuous'[146] link to a privacy policy,[147] and brokered an agreement with major app

---

[142] Ira S Rubinstein, 'Regulating Privacy by Design' (2011) 26 *Berkeley Tech LJ* 1409–1546 at 1433–1434.
[143] *United States v. W3 Innovations LLC* Case No CV–11–03958 (ND Cal Aug 12, 2011). The facts set out in this summary are drawn from the FTC complaint.
[144] A study in 2011 by Truste and Harris Interactive found that only 5% of all mobile apps had a privacy policy. In the 340 top free apps only 19% had a privacy policy. The study findings are reported by the California AG in State of California Office of the Attorney General.
[145] E.g. social networking and photo sharing apps Path and Hipster would automatically upload a user's entire address book without consent (to enable 'friend-finding' functions). Path apologised and began using opt-in consent. Parker Higgins, 'A Better Path for Apps: Respecting Users and Their Privacy' (*Electronic Frontier Foundation*, 8 February 2012) <https://www.eff.org/deeplinks/2012/02/better-path-apps-respecting-users-and-their-privacy> accessed 6 March 2020.
[146] The Online Privacy Protection Act of 2003, Cal. Bus. & Prof. Code §§ 22575–22579 (2004) s 22575 requires that 'an operator of a commercial web site or online service that collects personally identifiable information through the Internet about individual consumers residing in California who use or visit its commercial web site or online service shall conspicuously post its privacy policy.'
[147] State of California Office of the Attorney General.

marketplaces to facilitate this.[148] In terms of the consent order, the defendants were jointly and severally ordered to pay a civil penalty of $50 000, delete all information already collected from children, and report on COPPA compliance to the FTC.

However, even when a website or online service does have a privacy policy, it may not comply with COPPA. Xanga.com was a website offering a blogging service funded by behavioural advertising, targeting users of free accounts and a premium subscription service. A registration form was completed online by supplying an email address, username and password, and checking two boxes next to the statements:

'"I am at least 13 years old (no?)" (the "age box").

"I agree to Xanga Terms of Use" (the "terms of use" box).'[149]

If a user did not check the boxes before clicking 'create account' a pop-up displayed. In the case of the age box being left unchecked, the notification read: 'You must check the box below to certify that you are at least 13 years old'.[150] If a child under 13 checked the age box, they were then required to supply additional account information, including date of birth.

Children had entered their correct dates of birth and Xanga thus had actual knowledge that 1.7 million accounts had been created by children, but took no steps to delete the accounts. On the contrary, it collected personal information and permitted children to post public blog entries. Account information included first and last names, gender, metro (that is, major metropolitan area), state, ZIP code, country, mobile phone number, IM identifier, pictures uploaded by the child and information entered by the child under the fields '"about me', 'interests' and 'expertise'.

---

[148] State of California Office of the Attorney General, *Agreement to Strengthen Privacy Protections for Users of Mobile Applications*. The agreement was reached with Amazon, Apple, Google, Hewlett-Packard, Microsoft and Research In Motion (Blackberry). They agreed to create a field for app developers to provide information about their privacy policies or a hyperlink to their privacy policy when submitting apps to the app store. These fields were optional, but the agreement was an important milestone in making it easier for developers to communicate their app's practices to consumers.

[149] *United States v Xanga.com Inc* Case No 06–CIV–6853 (SDNY Sept 11, 2006). Save where otherwise indicated all facts are drawn from the FTC complaint.

[150] Ibid.

Xanga relied on inadequate means to provide notice of its information collection, use and disclosure practices, means which were not clear, understandable and complete, as required by COPPA. First, the "no?" next to the age box linked an explanation:

> *'"Sorry, Xanga is intended for people who are at least 13 years old. Children under 13 are not permitted to join or participate in the Xanga Community. Sorry for any inconvenience … please feel free to come back on your thirteenth birthday :-)".* '[151]

There was also a link on the registration page to Xanga's Terms of Use, which contained the following disclaimer:

> *'"You hereby certify to Xanga that you are at least 13 years old. Xanga is intended for people who are at least 13 years old. Children under 13 are not permitted to join Xanga or participate in the Xanga Community."* '[152]

This information was not displayed prominently and would not stand out in the body of the privacy policy.[153] Furthermore, it did not explain what information was collected, what it was used for and how it was shared with advertisers. Moreover, no direct notice was sent to parents and no steps were taken to obtain verified parental consent. Xanga.com (and its owner as second defendant) were fined $1 000 000 and were required to delete all children's information, and report to the FTC on COPPA compliance.

RockYou! operated a website that made available free 'widgets'.[154] For example, one widget enabled users to create slideshows from their photographs and share them

---

[151] Ibid. More recently in August 2016 hackers gained access to the personal information of 2,125,000 users, including 245,000 children, of iDress-Up, an online games and blogging website directed at children. I Dress-Up automatically sent parents an email if a user registered with a birthdate under 13, but even if parental consent was not received, the child could continue using the site in 'Safe Mode' indefinitely. Although the interactive blogging features were not available in safe mode iDress-Up still collected personal information (child's user name, password, birthdate, gender and email address as well as parent's email address). IDress-Up violated COPPA by not drafting a complete notice to parents (as there was no hyperlink to a comprehensive privacy policy), by not deleting all personal information if parental consent was not received, and by not adequately safeguarding the information. A civil penalty and compliance monitoring measures were imposed in the consent order. *United States of America v Unixiz Inc and others* Case No 5:19-cv-2222 (ND Cal Apr 24, 2019).

[152] *United States v Xanga.com Inc*.

[153] The link must be prominent and clearly labelled on the landing screen of the app, and each screen where personal information is collected. A small link in blue text at the bottom of a screen or webpage, or amongst other links, does not comply. See In *United States v V Tech Electronics Ltd and VTech Electronics North America LLC* Case No 1:18-cv-114 (ND Ill Aug 1, 2018)).

[154] In computing a widget is 'an element of a graphical user interface (GUI) that allows the user to interface with the operating system or an application [or it can refer to] the small program that is written to describe [how the widget functions]' E.g. a weather widget can display current weather on a smartphone's home screen but is in fact communicating with an app that is running in the background. Widgets include icons, counters, buttons, dialog

on social media networks. Users could choose to create an account to store their content, and were required to supply their email account name and password (which in itself was an unnecessary collection of personal information). They were later prompted to change this, but could re-enter the same password. A hacker gained access to 32 million account names and passwords (exposing the users' photographs in their RockYou! account and their email accounts, where the same password was used).

Typically, terms of service contain a representation about the security of the system but purport to exclude liability, and RockYou! adopted this approach in its own privacy policy:

> *'"RockYou!" uses commercially reasonable physical, managerial, and technical safeguards to preserve the integrity and security of your personal information. We cannot, however, ensure or warrant the security of any information you transmit to RockYou! and you do so at your own risk.'*[155]

boxes, pop-up windows, and toggle switches. Also see 'Difference Between App and Widget' (11 April 2018) <http://www.differencebetween.net/technology/difference-between-app-and-widget/> accessed 6 March 2020.

[155] *United States v RockYou Inc* Case No 3:12–cv–01487–SI (ND Cal Mar, 27, 2012). Save where otherwise indicated all facts are drawn from the FTC complaint.

Contrary to this representation, RockYou! failed to implement reasonable security measures in that:

a) RockYou! stored personal information (including email account passwords) in clear text.[156]

b) RockYou! failed to segment its servers (once a hacker infiltrated its network, he or she was able to access all information on the servers).[157]

c) At the time 'Structured Query Language' (SQL) injection and 'Cross-Site Scripting' (XSS) attacks were well-known and well-publicised threats. RockYou! failed to stay informed and failed to implement the readily available and inexpensive solutions that existed to prevent such attacks.[158]

d) To this (although this was not listed in the complaint), one could add that RockYou! evidently did not conduct vulnerability and penetration testing, use intrusion detection tools, or monitor logs to identify potential security incidents.[159] Recent enforcement actions have indicated that operators should use reasonable security measures such as firewalls, reverse proxies, strong cryptographic algorithms and Transport Layer Security (TLS) with up-to-date TLS certificates to protect personal information in transit and in storage and provide adequate training to employees.[160]

e) Furthermore, all operators of websites and online services should document, in writing, the content, implementation and maintenance of their information security programs.[161] The elements of such a program would include designating an appropriate employee(s) to oversee the program, regularly assess internal and

---

[156] Ibid.
[157] Ibid.
[158] Ibid.
[159] In 2019 the FTC took action against operators of two online services for inter alia failure to implement adequate security safeguards. See *United States of America v Unixiz Inc and others*. and *In the matter of James v Grago, Jr. doing business as ClixSense.com* FTC Dkt No C-4678 (Jul 2, 2019) (consent order).
[160] *In the matter of James v Grago, Jr. doing business as ClixSense.com* (complaint para 8). Also see *United States v V Tech Electronics Ltd and VTech Electronics North America LLC*. Personal information entered on the Learning Lodge website was transferred to the defendant's servers in plain text contrary to an assurance in its privacy policy that 'In most cases, if you submit your PII [personally identifiable information] to VTech directly through the Web Services it will be transmitted encrypted to protect your privacy using HTTPS encryption technology.' On its servers passwords and children's photos and audio files were stored in an encrypted format, but the decryption key was stored in the same database, and the data was linked to parent's data so that e.g. a hacker could associate a child's photo with the physical address supplied by their parent.
[161] *In the matter of James v Grago, Jr. doing business as ClixSense.com*.

external risks, and identify, implement, test and monitor safeguards appropriate to the risk and sensitivity of the information collected.[162]

RockYou! also included a warning in its privacy policy that children under 13 were not to use the site.

> *'Our Commitment to Children's Privacy: Protecting the privacy of young children is especially important. For that reason, RockYou! does not knowingly collect or maintain personally identifiable information or non-personally-identifiable information on the RockYou! Sites from persons under 13 years of age, and no part of our website is directed to persons under 13. If you are under 13 years of age then please do not use or access the RockYou! Sites at any time or in any manner. If RockYou! learns that personally identifiable information of persons under 13 years of age has been collected on the RockYou! Sites without verified parental consent, then RockYou! will take appropriate steps to delete this information.'*[163]

However, RockYou! had actual knowledge that 179 000 children had created accounts because account holders were required to supply a birth year. RockYou! took no steps to give notice to parents or obtain prior parental consent, or to delete information obtained from children without this consent.

The FTC imposed a civil penalty of $250 000, and an injunction to comply with COPPA and delete all personal information of children already collected. However, in a departure from early orders requiring self-reporting on COPPA compliance for a fairly limited period,[164] RockYou! were required to appoint an independent, qualified professional to implement a privacy program and send an initial and biennial compliance reports to the FTC for 20 years.

Further, for a period of five years, RockYou! were required to display a prominent notice and hyperlink on its website and online services directed at children to OnGuard, the parent's section of the FTC's consumer education portal.[165]

---

[162] Ibid (consent order).
[163] *United States v RockYou Inc*.
[164] E.g. in 2008 in *United States v Industrious Kid Inc* Case No CV–08–0639 (ND Cal,filed Jan 28, 2008) and 2011 in *United States v. W3 Innovations LLC* annual reports by the operator to the FTC were required for 3 years only, and documentation proving compliance had to be available for inspection for 3 years, and each document retained for 2 years after its creation.
[165] Similar provisions were included in consent orders from around 2006. See *United States v Xanga.com Inc*.

Most recently the FTC imposed its largest fine of an app developer to date, when it fined the developers of the TikTok app $5 700 000.00.[166] The consent order imposes annual self-reporting and record-keeping in relation to COPPA compliance for 10 years.

TikTok is a wildly popular free social app for Android and iPhone[167] that allows users to create and post short videos lip-syncing to popular music, and has a number of interactive features.[168] Adults had used the app to contact children,[169] as it permits direct messaging between users, and until 2016 also included a city 'directory' of nearby users.[170] To create an account, users were required to supply an email address, phone number, full name, username, a profile picture, and personal 'bio'.[171] By default, the account was public and direct messaging between users was enabled. Even when privacy settings were altered by the user, the user's 'bio', profile picture and username would remain public and fully searchable.[172]

In December 2016 a media interviewer publicly alleged that popular TikTok accounts were held by children. TikTok then identified 46 of its most popular accounts were held by children but instead of closing the accounts, it sent the users an email instructing them to edit their profile description to indicate that their accounts were being run by a parent or adult talent manager. It took no steps to ensure that this was the case or that a parent had received the email.[173]

---

[166] *United States of America v Musical.ly* Case No 2:19-cv-01439 (CD Cal Feb 27, 2019) (proposed consent order)

[167] Save where indicated to the contrary, the facts of this summary are drawn from the FTC complaint filed of record in ibid. At the date of the complaint TikTok had 200 million downloads and 65 million account holders in the US alone. During the time period with which the FTC complaint is concerned the app was known as Musical.ly app. After ByteDance Ltd (of Beijing) acquired Musical.ly in December 2017 the app was merged (in August 2018) with TikTok.

[168] The TikTok app preview on Google Play store. Available at 'https://play.google.com/store/apps/details?id=com.zhiliaoapp.musically&hl=en_ZA'. Accessed on 29 August 2019.

[169] Fair L 'Largest FTC COPPA settlement requires Musical.ly to change its tune' (27 Feb 2019). Available at 'https://www.ftc.gov/news-events/blogs/business-blog/2019/02/largest-ftc-coppa-settlement-requires-musically-change-its'. Accessed on 29 August 2019.

[170] *United States of America v Musical.ly* , complaint para 18: 'Until October 2016, the App had a feature where a user could tap on the "my city" tab, which provided the user with a list of other users within a 50-mile radius, and with whom the user could connect and interact with by following the user or sending direct messages.'

[171] Ibid. Although the app later introduced an age restriction existing user accounts were not screened to exclude children.

[172] Ibid.

[173] *United States of America v Musical.ly* complaint para 22. Also see *United States v Prime Sites Inc.* Case No 2:18-cv-00199 (D Nev May 2, 2018) concerning a talent search website that permitted users under 13 to register. Its privacy policy stated 'If you are a child under the age of 13, your profile must be created by a legal guardian. No one under age 13 may provide any information to or through [ExploreTalent.com]. We do not knowingly collect personal information from children under 13.' However the operator took no steps to verify that children's

Unlike the online services of Xanga and RockYou!, the TikTok app did not collect a user age as part of the account registration process before July 2017.[174] However, the app developers had actual knowledge that there were many users under 13, not only because of the media-sparked investigation referred to above, but when taking into account its own privacy statements,[175] information contained in user profiles (including pictures, age, or school), press reports, and 'thousands' of parents' complaints to the developer.[176] Moreover, on any assessment of the content of the app, it targeted children. Its online library contained songs popular with children and tweens, arranged by the developer in song folders such as "Disney" and "school", and the app provided tools and bright emoji characters that were easy to use and appealing to children.

VIII REGULATORY ENFORCEMENT ACTION AGAINST YouTube

YouTube, a wholly owned subsidiary of Google, is a video-sharing platform on the internet and a mobile application where users can view, upload, comment on and share video content.[177] YouTube has developed an age classification tool that rates some content as suitable for children. In 2015, 'YouTube Kids' was launched for children aged 2 to 12. This site does not collect personal information and delivers only contextual advertising. The defendants' automated filters take content that is age-rated for children from YouTube, and the YouTube kids home 'canvas' features a list of recommended channels manually curated by the defendant's employees. However, child-directed content remains available on YouTube, and at no point has Google or YouTube attempted to prevent children under 13 from viewing YouTube without verified parental consent.[178]

---

profiles were in fact being created by a legal guardian. It was fined $500 000 (of which $265 000 was suspended) and subject to reporting requirements for 20 years.

[174] From July 2017 the app requires users to enter their age and does not permit users under 13 to create an account. However bypassing this only requires entering a false birthdate. TikTok has a section for younger users, and a privacy policy for younger users, however this appears to be enforced only in respect of US resident children.

[175] Its website stated 'If you have a young child on Musical.ly, please be sure to monitor their activity on the App'.

[176] *United States of America v Musical.ly* - If parents complained the developer closed the accounts but they did not delete the users' videos or profile information from Defendants' servers, and took no action to close other child accounts.

[177] *United States of America and People of the State of New York v Google LLC and YouTube LLC* Case No 1:19-cv-02642 (DDC Sep 10, 2019) (draft consent order). This summary of the facts is drawn from the Revised Complaint (para 16–41).

[178] In reality this means children could open the site or the mobile app and be automatically logged in under their parent's account.

Users can upload content if they have created a Google account and a YouTube "channel". As the channel owner, they then choose key words to direct traffic to their site and to specific videos and elect whether to permit comments. The channel owners and YouTube earn revenue from behavioural advertising in YouTube and through retargeting on other websites.[179]

Google and YouTube are deemed to be operators of a 'child directed' website or service as they have 'actual knowledge' that they are collecting personal information (advertising identifiers) directly from the user of child-directed YouTube channels.[180] A number of relevant factors pointed to the conclusion that YouTube was a child-directed website,[181] and the approach is similar to that applied in earlier enforcement actions.[182] YouTube were required to pay a combined civil penalty of US$ 170 000 000 to the FTC and the State of New York.[183]

Although channel owners may not collect any personal information themselves, they are also deemed to be 'operators' as they permit Google and YouTube to collect personal

---

[179] *United States of America and People of the State of New York v Google LLC and YouTube LLC*. From January 2016 channel owners were given the option to disable behavioural advertising (but this setting comes with a warning that the site will earn lower revenue as it can then only deliver contextual adverts). The complaint does not refer to any warnings given by YouTube to channel owners on COPPA compliance, and is critical of training documents available on YouTube which used YouTube channels (that did not comply with COPPA) as references for creating 'family friendly' content.

[180] Children's Online Privacy Protection Rule, 16 C.F.R part 312 (COPPA Rule), definition of 'Website or online service directed at children'.

[181] *United States of America and People of the State of New York v Google LLC and YouTube LLC*. The complaint asserted that the subject matter and content of the channels was clearly child-directed: e.g. toy reviews, cartoons, fun family skits, and nursery rhymes. This was further reflected in channel names, video titles, channel descriptions under the 'about section' (e.g. 'made just for kids!) and key words that the channel owners had configured to direct traffic to their channel and specific videos (e.g. 'kids cartoons'). Channels features popular animated characters and child presenters. YouTube's age rating tool and marketing materials recognised the content as pertaining to children. Content from these channels regularly appeared on YouTube Kids, or on the curated YouTube Kids home screen and in several cases at least one video appearing on the channels referred to in the complaint was one of the most popular videos on YouTube Kids during a 90-day period in 2016. By analogy in the context of mobile apps, app stores give app developers the means to categories their games as made for kids, and provide information about the app in the app store in addition to the app's promotional material on the developer's website.

[182] See e.g. *United States v. W3 Innovations LLC*) where the app 'Emily's Girl World' (and related 'Emily' apps) contained games and an interactive blog that appealed to the developer's target demographic of elementary school girls. The app was listed in the 'Games- Kids' section of Apple's app store, and was described in promotional material on the developer's website as 'a fun story-telling app with charming graphics ... which we thought that younger girls and nostalgic adults in particular might enjoy.' In terms of a consent order the developers agreed to pay a civil penalty of $50 000, delete all children's information already collected, and submit compliance reports to the FTC for 3 years.

[183] *United States of America and People of the State of New York v Google LLC and YouTube LLC* (Stipulated Order for Permanent Injunction and Civil Penalty Judgment).

information on their behalf (in that the channel owner benefits from the advertising revenue this generates).[184] Channel owners must comply with COPPA in relation to child-directed content, failing which they, too, would be subject to regulatory action including civil penalties.

IX CLASS ACTION AGAINST ZOOM VIDEO COMMUNICATIONS INC

The California Consumer Privacy Act (CCPA)[185] came into force on 1 January 2020. In March a class action was launched against the developers of Zoom, a massively popular online conferencing website and mobile application, alleging that the iOS version of the app shared personal information with Facebook in breach of the CCPA.[186]

As noted from the earlier studies discussed in chapter 5,[187] and a recently published industry report on Zoom,[188] the Facebook SDK (which is integrated by app developers to allow app users to login to an app with their Facebook login if they do not want to create a separate account) will collect data from all app users (even if they do not have a Facebook account or do not log in using their Facebook credentials). Facebook receives notification each time the app is opened, and device information that enables the delivery of targeted advertising, including device model, OS type and version, language setting, time zone, carrier, processing core and disk space and an advertising identifier (a form of unique identifier that permits linking of activity on different websites and apps on one device).[189] As discussed in chapter 4, this is personal information under the CCPA and is being 'sold' to a third party, as those terms are used in the CCPA.[190] The disclosures in Zoom's privacy policy do not clearly address the sharing with Facebook from the app itself, and the 'Do Not Sell My Personal

---

[184] COPPA Rule 16 C.F.R §312, definition of 'operator'.
[185] The California Consumer Privacy Act of 2018, Cal. Civ. Code §§ 1798.100 - 1798.199 (CCPA).
[186] *Robert Cullen, individually and on behalf of all others v Zoom Video Communications Inc.* Case No 5:20-cv-02155 (ND Cal, Mar 30, 2020).
[187] See the discussion in chapter 5 of *Wirtschaftsakademie Schleswig-Holstein* (C-210/16) ECLI:EU:C:2018:388 a case which concerned the use of Facebook's advertising tools on a business fan page, and the reference to Privacy International, *How Apps on Android Share Data with Facebook (even if you don't have a Facebook account)* (2018) and Reuben Binns and others, 'Third Party Tracking in the Mobile Ecosystem' in *Proceedings of the 10th ACM Conference on Web Science* (ACM, Amsterdam, Netherlands 27–30 May 2018).
[188] Joseph Cox, 'Zoom iOS App Sends Data to Facebook Even if You Don't Have a Facebook Account' (*Vice Tech*, 26 March 2020) <https://www.vice.com/en_us/article/k7e599/zoom-ios-app-sends-data-to-facebook-even-if-you-dont-have-a-facebook-account> accessed 4 April 2020.
[189] *Robert Cullen, individually and on behalf of all others v Zoom Video Communications Inc.* para 16. Also see the limited admission in Erik S. Yuan, 'Zoom's Use of Facebook's SDK in iOS Client' (*Zoom Blog*, 2020) <https://blog.zoom.us/wordpress/2020/03/27/zoom-use-of-facebook-sdk-in-ios-client/> accessed 4 April 2020.
[190] CCPA §1798.140(t)(1).

Information' link required by the CCPA was restricted to Zoom's marketing website and not offered to app users for the sharing of data with Facebook.[191]

Zoom has since changed the feature,[192] but given that this was widely reported over a year ago[193] and that bug reports about the feature have been filed on Facebook's developer forum since 25 May 2018,[194] Zoom's claim that they did not know about the data-sharing feature of the Facebook SDK is unlikely to absolve them from legal liability. In the SDK v4.34, developers have the option of delaying the automatic logging of events until after they have collected consent.[195] It appears that Zoom did not obtain CCPA-compliant consent at all. Furthermore, Facebook did not obtain consent in that, although users with a Facebook account are bound by Facebook's privacy policy and its terms and conditions related to data sharing,[196] Facebook has no user consent to receive personal information about users who do not have a Facebook account.[197]

---

[191] *Cullen v Zoom Video Communications Inc* para 16. Also see Zoom, 'Privacy Policy' <https://zoom.us/privacy> accessed 4 April 2020, which contained the following relevant terms:
'Linked Websites and Third-Party Services
Our marketing websites may provide links to other third-party websites and services which are outside our control and not covered by this policy. We encourage you to review the privacy policies posted on these (and all) sites you visit or services you use.
Does Zoom sell Personal Data?
We do not sell your data.
We do not allow marketing companies, advertisers or similar companies to access personal data in exchange for payment. We do not allow third parties to use any personal data obtained from us for their own purposes, unless you consent (e.g., when you download an app from the Marketplace).
…
As described in the Zoom marketing sites section, Zoom does use certain standard advertising tools on our marketing sites which, provided you have allowed it in your cookie preferences, sends personal data to the tool providers, such as Google. This is not a "sale" of your data in the sense that most of us use the word sale. However, California's CCPA law has a very broad definition of "sale". Under that definition, when Zoom uses the tools to send the personal data to the third-party tool providers, it may be considered a "sale". It is important to know that advertising programs have always worked this way and we have not changed the way we use these tools. It is only with the recent developments in data privacy laws that such activities may fall within the definition of a "sale".
Because of CCPA's broad definition, as is the case with many providers since the CCPA became law, we provide a "Do Not Sell My Personal Information" link at the bottom of our marketing sites. You can use this link to change your Cookie Preferences and opt out of the use of these advertising tools. If you opt out, Personal Data that was used by these tools will no longer be shared with third parties in a way that constitutes a "sale" under CCPA.'
[192] Yuan op cit note 189.
[193] Privacy International op cit note 187.
[194] Ibid at 4.
[195] Ibid.
[196] Facebook Inc., 'Data Policy' (19 April 2018) <https://www.facebook.com/about/privacy> accessed 26 October 2019.
[197] Similarly see *Wirtschaftsakademie Schleswig-Holstein* discussed in chapter 5.

There are further concerns about the collection of communications content and security measures adopted by Zoom,[198] with reports of 'Zoombombing',[199] and reports that the app 'leaks' emails and photographs and permits strangers to initiate a zoom call to app users.[200] These reports call into question the accuracy of Zoom's assertion that they use 'industry standard' security measures to protect privacy.[201]

COPPA, GDPR, POPIA and GDPR all require app developers to be up-to-date with the technological and organisational measures reasonable for ensuring security, integrity and *confidentiality* of personal information.[202] However, only COPPA imposes an obligation to transfer data to third parties only when they also maintain adequate safeguards.[203]

The allegations in this action illustrate that even when apps are processing personal information on a large scale, they are not necessarily taking steps to implement adequate data protection in relation to the security and confidentiality of the personal information that they process.

---

[198] The class action does not allege that Zoom shared content or metadata about communications made on the app with Facebook. However questions arise about whether Zoom is recording conference calls, and how it is protecting and using this information. These questions have been addressed to Zoom in a letter from the New York Attorney General as reported in Danny Hakim and Natasha Singer, 'New York Attorney General Looks Into Zoom's Privacy Practices' *New York Times* (30 March 2020) <https://www.nytimes.com/2020/03/30/technology/new-york-attorney-general-zoom-privacy.html> accessed 4 April 2020.

[199] The term 'zoombombing' arose in 2020 when conference calls using Zoom were intercepted by hackers who displayed pornography, profanities and hate speech such as Nazi propaganda to the meeting participants. Editorial, 'Zoom Slapped with Class Action Lawsuit over Facebook Data-sharing Issues' *Engineering & Technology* (1 April 2020) <https://eandt.theiet.org/content/articles/2020/04/zoom-slapped-with-class-action-lawsuit-over-facebook-data-sharing-issues/> accessed 4 April 2020.

[200] Joseph Cox, 'Zoom is Leaking Peoples' Email Addresses and Photos to Strangers' (*Vice Tech*, 1 April 2020) <https://www.vice.com/en_us/article/k7e95m/zoom-leaking-email-addresses-photos> accessed 4 April 2020. Zoom's 'company directory' setting automatically adds other people to a user's list of contacts (including email address and profile pic) when their email address includes the same domain. This is a useful feature for users in the same company, but it was enabled by default meaning users who signed up with a private email address were sharing their contact details with 1000s of strangers using the same domain. Although it excludes large public domains such as Gmail, Yahoo and Hotmail, it was not set up to detect domains of internet service providers (ISPs) which offer email services. This is something the ISP cannot disable.

[201] Zoom. The privacy policy provides:

'Security of your Personal Data

Zoom is committed to protecting your personal data. We use a combination of industry-standard security technologies, procedures, and organizational controls and measures to protect your data from unauthorized access, use, or disclosure.'

[202] CCPA requires a covered business to 'implement and maintain reasonable security procedures and practices' and § 1798.150 subjects a business to civil actions for damages and injunctive or other relief if they fail to so and the 'nonencrypted and nonredacted' personal information is subject to unauthorized access, theft or disclosure.

Cf Children's Online Privacy Protection Rule, 16 C.F.R part 312 (COPPA Rule) §312.3(e) & §312.8; GDPR art 5(1)(f), 24 & 32; and POPIA s 19.

[203] COPPA Rule 16 C.F.R §312.8.

However, the allegations in the class action also point to a deeper issue that lies at the heart of this dissertation: an accountability gap that makes PbD unenforceable under current legislative frameworks.

First, app developers are not informing themselves about privacy threats in the third party code that they integrate, and in the privacy (including security) practices adopted by those third parties. From a PbD perspective, Zoom have failed to be 'proactive' about privacy, despite their claims to take privacy 'extremely seriously',[204] they have failed to institute privacy as the 'default' setting, and they have failed to keep privacy 'user-centric' and 'user-friendly'.

Secondly, PbD is premised upon proactive privacy measures being adopted not only throughout an organisation but also throughout an ecosystem. As discussed in chapter 5, Facebook would be regarded as a controller in relation to the information received, as it has designed the means and the purpose of processing. It must be possible for Facebook to design their 'login with Facebook' SDK in such a way that it will collect data only from Facebook users, or users who have given consent to the collection. Despite developer complaints to Facebook that its SDK makes it impossible for developers to comply with the requirement for consent *prior* to any collection,[205] and intense judicial and regulatory scrutiny,[206] Facebook appears to have maintained the view that it is the responsibility of the app developer to obtain consent for this data sharing.[207]

---

[204] Yuan.
[205] As required by GDPR (and COPPA and POPIA).
[206] See e.g. *Wirtschaftsakademie Schleswig-Holstein In the Matter of Facebook Inc* and *United States v Facebook Inc* Case No 1:19-cv-02184, related FTC Dkt No C-4365 (DDC Jul 24, 2019) (consent order).
[207] Facebook Inc., 'Facebook Platform Policy' <https://developers.facebook.com/policy/> accessed 26 October 2019 provides:
'Obtain adequate consent from people before using any Facebook technology that allows us to collect and process data about them, including for example, our SDKs and browser pixels. When you use such technology, provide an appropriate disclosure:
. a. That third parties, including Facebook, may use cookies, web beacons, and other storage technologies to collect or receive information from your websites, apps and elsewhere on the internet and use that information to provide measurement services, target ads and as described in our DATA POLICY; and
b. How users can opt-out of the collection and use of information for ad targeting and where a user can access a mechanism for exercising such choice.'
This in turn refers developers to the device settings for limiting ad tracking (which as explained in chapter 2 depend upon device model and OS type and version and are created by device manufacturers and OS platform providers.)
The policy also provides in relation to COPPA compliance:

Zoom have solved the problem by removing Facebook's SDK from the latest version of the iOS app (although users who continue using an older version will not be protected). In the case of small app developers, however, it may not be possible for them to create the code necessary to permit a Facebook login (and pass Facebook's app review process), and this could prejudice users even further as the earlier discussion of weak security practices by app developers in relation to their collection and storage (in unencrypted form) of account details and passwords showed. As a study of close to one million free Android apps showed, this kind of data sharing is ubiquitous.[208] Over 80% of the apps in the study were embedded with third party trackers; 42% of these apps share data with Facebook, and over 88% of the apps share data with Alphabet (the Google parent company and its subsidiaries). If one considers only Facebook's own disclosures to user about its collection of personal information from products and services that integrate with Facebook, it is clear that the principle of data minimisation is not being effectively implemented.[209]

'Web sites or services directed to children under 13: If you use Social Plugins or our JavaScript SDK for Facebook on sites and services that are directed to children under 13, you are responsible for complying with all applicable laws.'

[208] Binns and others.

[209] Facebook Inc., 'Data Policy'. The privacy policy records:

'Device information.

As described below, we collect information from and about the computers, phones, connected TVs and other web-connected devices you use that integrate with our Products, and we combine this information across different devices that you use. …

- Device attributes: operating system, hardware and software versions, battery level, signal strength, available storage space, browser type, app and file names and types, and plugins,
- Device operations: information about operations and behaviours performed on the device, such as whether a window is foregrounded or backgrounded, or mouse movements (which can help distinguish humans from bots).
- Identifiers: unique identifiers, device IDs and other identifiers, such as from games, apps or accounts that you use, and Family Device IDs (or other identifiers unique to Facebook Company Products associated with the same device or account).
- Device signals: Bluetooth signals, information about nearby Wi-Fi access points, beacons and mobile phone masts.
- Data from device settings: information that you allow us to receive through device settings that you turn on, such as access to your GPS location, camera or photos.
- Network and connections: information such as the name of your mobile operator or ISP, language, time zone, mobile phone number, IP address, connection speed and, in some cases, information about other devices that are nearby or on your network, so we can do things such as help you stream a video from your phone to your TV.
- Cookie data: data from cookies stored on your device, including cookie IDs and settings. Learn more about how we use cookies in the Facebook Cookies Policy and Instagram Cookies Policy.'

X CONCLUSION

This chapter has demonstrated that a PbD approach has been endorsed by the FTC and California AG in the US as a best practice approach, although it goes beyond the FIPPs of notice and consent and is not enforceable as a legal obligation under existing legislative frameworks in the US. A fortiori this provides an inadequate basis for implementing Pb(re)D through the re-design of existing hardware and software components, and data sharing practices within the mobile apps eco-system.

The robust record of regulatory enforcement actions and class action suits in the US make it clear that contractual disclaimers and limitations of liability will not protect an app developer who fails to comply with statutory obligations, nor will they assist an app developer where the privacy policy contains false and misleading misrepresentations to consumers about the developer's actual practices.[210] Thus, an app developer who has actual knowledge that it is collecting information from children cannot rely on a disclaimer that the service may not be used by children, or that children under 13 should be assisted by a guardian. Further app developers have a responsibility to implement security safeguards both in relation to the mobile app itself and the transfer and storage of data off the user's device, and do not escape liability if the vulnerability is introduced by third party code.[211]

---

[210] In the US failure to have a privacy policy that is clear, understandable and complete is a violation of the COPPA Rule and constitutes an unfair or deceptive act or practice in or affecting commerce, in violation of s 5(a)(1) of the FTC Act 15 U.S.C. § 45(a)(1), in terms of section 1303(c) of COPPA 15 U.S.C. § 6502(c), read with s 18(d)(3) of the FTC Act 15 U.S.C. § 57a(d)(3). See further *United States v Godwin* a social networking website for children with 5600 users, which took no steps to notify parents and obtain verified consent when children set up an account (contrary to representations in its privacy policy). It was fined $100 000 and ordered to appoint an independent professional privacy expert to report to the FTC for 5 years on the implementation of COPPA compliance measures.

[211] *In the matter of James v Grago, Jr. doing business as ClixSense.com* (facts summarised from complaint). Clixsense earned significant revenue by having its account holders view ads and take surveys. As explained in chapter 2, online advertising revenue is frequently calculated by the number of 'clicks' on an ad. Of its many security failures, the most egregious was that when Clixsense learned about a publicly available web browser extension that automatically clicked on ads, it downloaded the extension onto the Clixsense network. It took no steps to separate the software from its other systems. It also failed to secure employee's laptops on which user credentials and passwords were stored in plain text. Hackers exploited a vulnerability in the browser extension to infiltrate Clixsense's network and obtained access (through a compromised employee laptop) to an old server that Clixsense had not disconnected from its network. The personal information of 6.6 million consumers— of whom 500 000 were US residents, was stored on that server in plain text including sensitive information such as social security numbers, and answers to security questions, which exposed the affected consumers to a high risk of identity theft and fraud. As Clixsense made deceptive representations to its users that they employed 'the latest security and encryption techniques' to safeguard personal information the FTC took action under s 5 of the FTCA.

The action taken by the FTC against Google and YouTube indicates that it may pay even closer scrutiny to the accountability of platforms. However, the FTC takes the view that 'the COPPA Rule does not require platforms to actively screen content to determine if it is child-directed'.[212]

Similarly, the FTC has taken the view that COPPA was not intended to regulate app stores. It therefore does not regard app stores as accountable for the apps that are made available on its platform, although it remains to be seen whether an app store would be liable under section 5 of the Federal Trade Commission Act for failure to enforce its public app review guidelines and privacy policies against mobile app developers. Thus far the FTC has reported app violations to app stores and requested that they take down the apps.[213]

Therefore, a key weakness of the US approach is that beyond advocacy measures from regulators and industry associations, no mechanism exists to require compliance with a PbD approach by all role-players within the mobile app ecosystem.

Secondly, this chapter has demonstrated that regulatory guidance issued by data protection authorities cannot be restricted to a textual restatement of data protection principles. The key strength of the US approach lies in the use of multi-stakeholder processes to develop co-operative solutions around agreed industry standards. However, there remains a gap in relation to processing by third parties and the accountability of upstream technology and platform providers.

It is important that the voice of app developers is heard in this process. So far as their views have been canvassed, app developers view privacy as an engineering challenge:

> *'Achieving transparency about data collection and usage can be resolved with good design. Letting consumers know what is being collected and how it is being used is good user interface (UI). … No number of regulations or laws can actually improve the way*

---

[212] Federal Trade Commission, 'Statement of Joseph J. Simons & Christine S. Wilson Regarding FTC and People of the State of New York v. Google LLC and YouTube, LLC ' (4 September 2019) <https://www.ftc.gov/system/files/documents/public_statements/1542922/simons_wilson_google_youtube_statement.pdf> accessed 15 May 2020. But see the dissenting statement of Commissioner Slaughter.

[213] See e.g. FTC Commissioner Christine S. Wilson, 'The FTC's Role in Supporting Online Safety ' (Remarks at the Family Online Safety Institute, Washington DC, 21 November 2019) at 10 <https://www.ftc.gov/system/files/documents/public_statements/1557684/commissioner_wilson_remarks_at_the_family_online_safety_institute_11-21-19.pdf> accessed 9 March 2020. In 2019 the FTC sent notice to Ukrainian developer Wildec that three of its dating apps were not COPPA compliant, and sent notice to Apple and Google, who promptly removed the apps from the app stores.

apps treat consumers or their data. Laws, regulations and enforcements only can sanction failures – they do not enable developers to think outside of the box and innovate. "[214]

In chapter 4 it was noted that there are growing calls for a federal privacy statute. None of the draft bills presented to Congress include an express PbD article. However, if those bills contain the core data protection principles outlined earlier, provide a definition of personal information, and make app developers (and other parties processing personal information) legally accountable for the lawful collection, use and sharing of such information, then the PbD best practice recommendations can be implemented by enforcing the legislation. In short, the US approach illustrates that government regulation and industry self-regulation should be used together.

[214] Rachel Emeis, 'Preliminary Report from the 10-City Application Developers Alliance Privacy Summit Series' (29 November 2012) <https://www.developersalliance.org/press-releases/preliminary-report-from-the-10-city-application-developers-alliance-privacy-summit-series> accessed 2 March 2020. Also see European Union Agency For Network and Information Security.

CHAPTER 8

THE INCLUSION OF "PRIVACY BY DESIGN" IN THE EU GENERAL DATA PROTECTION REGULATION

I INTRODUCTION

Chapter 3 set out the foundational principles of Privacy by Design (PbD), and the development of the closely related concept of Privacy by (re)Design (Pb(re)D) which seeks to apply these principles through the redesign of existing technologies and system. Chapter 7 further examined the birth of PbD and its inclusion in regulatory guidelines in the US and other jurisdictions. The EU has taken the lead of introducing PbD as an explicit legal duty in article 25 of GDPR. This chapter will set out the background to that development and provide a critical analysis of article 25 and other amendments to GDPR to determine whether the express inclusion of PbD represents an approach that South Africa should follow. The position in South Africa will be discussed in the subsequent chapter.

II PbD IN THE EU BEFORE GDPR

As outlined in the previous chapter, the report from which the concept of PbD originated was not calling for the adoption of new additional principles of data protection. Nor was it saying that security is not an important aspect of preserving privacy.[1] The elements of a PbD approach were already provided for in the existing legal framework in Europe, and the Article 29 Working Party's opinion on apps in 2013 emphasised the importance of PbD and provided guidance on its application to role-players in the ecosystem.[2]

The 1995 Data Protection Directive[3] provided in article 17 (Security of Processing) that data controllers were to use 'appropriate technical and organisational measures

[1] As outlined in the quote above security becomes a 'paramount' concern once personal data has been collected.
[2] Article 29 Data Protection Working Party, *Opinion 02/2013 on apps on smart devices* (WP 202, 27 February 2013) at 11.
[3] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (Data Protection Directive) OJ 1995 L 281/31, 23.11.1995.

to protect personal data … [inter alia] against all other unlawful forms of processing'.[4] While the article was headed 'security', it encompassed in its reference to 'all other forms of unlawful processing' a reference to all the conditions of lawful processing set out in article 6 of the 1995 Directive (now article 5 of the GDPR).[5] In particular, the data protection principles of lawfulness, fairness, transparency, purpose limitation and storage limitation all support a PbD approach.[6] Recital 46 required that such measures be taken 'both *at the time of the design of the processing system* and at the time of the processing itself' (own emphasis), in other words, as early as possible.[7] Since by definition processing extends to 'any operation or set of operations which is performed upon personal data'[8] from the earliest moment (collection), throughout the duration of its storage, use, retrieval or transmission and until the last moment (erasure or destruction), this encompassed the notion of 'full-lifecycle protection' envisaged by PbD.[9] Further, article 16 imposed a requirement for confidentiality on processors (but did not address other role-players in the ecosystem such as technology, platform providers and third parties).[10]

It should further be noted, with specific reference to digital technologies and mobile apps in particular, that the e-Privacy directive[11] does not explicitly refer to PbD.[12] However, it empowers EU member states to adopt measures 'where required' to ensure that

---

[4] The article also requires data controllers to use contractual means to ensure the processors provide sufficient guarantees that such measures will be implemented. The article, and the similar provisions in POPIA and GDPR will be considered in detail later in relation to accountability.

[5] Cf Aurelia Tamò-Larrieux, *Designing for Privacy and its Legal Framework –Data Protection by Design and Default for the Internet of Things* (Springer 2018) who suggests that art 25 has broadened the scope of the privacy by design requirement which was restricted under the 1995 Data Protection Directive to security.

[6] Article 29 Data Protection Working Party and Working Party on Police and Justice, *The Future of Privacy: Joint contribution to the Consultation of the European Commission on the Legal Framework for the Fundamental Right to Protection of Personal Data* (WP168, 1 December 2009) at 13.

[7] Ibid at 14.

[8] Data Protection Directive 95/46/ECart 2(b).

[9] Cf Tamò-Larrieux who suggests that under the 1995 Directive the implementation of appropriate technical and organisational measures was restricted to the 'initial design phase' and has been broadened by art 25 to apply to the full lifecycle of the data. She overlooks the requirement of continuous monitoring and improvement of security safeguards.

[10] Article 29 Data Protection Working Party and Working Party on Police and Justice at 13.

[11] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector 2002/58/EC (e-Privacy Directive) OJ L 201/37, 31.7.2002.

[12] Ibid rec 30 specifies that '[s]ystems for the provision of electronic communications networks and services should be designed to limit the amount of personal data necessary to a strict minimum...' and rec 46 provides that '[t]he protection of the personal data and the privacy of the user of publicly available electronic communications services should be independent of the configuration of the various components necessary to provide the service.'

the construction of terminal equipment is compatible with user privacy.[13] This has not been done. Likewise, the radio equipment directive of 2014,[14] and the now repealed 1999 Radio and Telecommunication Terminal Equipment Directive,[15] empower the European Commission to decide that certain categories or classes of radio equipment must implement privacy safeguards.[16] As no such decision has been issued, the provision does not apply.[17] The draft e-Privacy Regulation also makes no reference to PbD.[18]

In short, adequate legal principles already existed to compel a PbD approach but, as a result in part of fragmentation arising from the disparate implementation of the 1995 Directive, and in part of the failure to develop technical standards applicable to terminal equipment and radio equipment manufacturers, those principles were not being effectively and consistently enforced.[19]

---

[13] Ibid art 14. ’

[14] Directive 2014/53/EU of the European Parliament and of the Council of 16 April 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of radio equipment and repealing Directive 1999/5/EC OJ L 153/62, 22.5.2014 (RE-Directive) (RE-D). The RE-D became effective on 12 June 2016 and all equipment launched on the market after the end of the transitional period on 12 June 2017 had to comply with the new directive.

[15] Directive 1999/5/EC of the European Parliament and of the Council of 9 March 1999 on radio equipment and telecommunications terminal equipment and the mutual recognition of their conformity OJ L 91/10, 7.4.1999 (RTTED).

[16] RE-D art 3(3)(e) provides:

‘Article 3

Essential requirements

…

3. Radio equipment within certain categories or classes shall be so constructed that it complies with the following essential requirements:

…

e) radio equipment incorporates safeguards to ensure that the personal data and privacy of the user and of the subscriber are protected;

…

The Commission shall be empowered to adopt delegated acts in accordance with Article 44 specifying which categories or classes of radio equipment are concerned by each of the requirements set out in points (a) to (i) of the first subparagraph of this paragraph.’

[17] There is currently no delegated act on art 3(3)(e) nor was there any decision under art 3(3)(c) of the RTTED. Also see Article 29 Data Protection Working Party and Working Party on Police and Justice at 15 (para 54–56) and Article 29 Data Protection Working Party at 11.

[18] Proposal for a regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic
communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) Brussels, 10.1.2017 COM(2017) 10 final 2017/0003 (COD). There is no equivalent of rec 30 requiring the design of systems to limit collection to a ‘strict minimum’.

[19] European Data Protection Supervisor (EDPS), *Opinion of the European Data Protection Supervisor on Promoting Trust in the Information Society by Fostering Data Protection and Privacy* (2010) recommendations at 8.

III BACKGROUND TO THE ADOPTION OF PbD INTO GDPR

In the light of the above observations, the prevailing view, at least at the initial stages of law reform discussions, was that PbD went beyond the requirements of legislation based on FIPs, but that in Europe it was an approach that could help organisations to comply with their existing data protection obligations under the 1995 Directive. This began to change with calls from around 2009 for the introduction of PbD as an 'additional principle' into the European data protection legislation.[20] At this point, there was a decided shift from the earlier view that a PbD approach could be achieved through alternative policy instruments[21] such as sector-specific guidance on technologies.[22] The premise of these calls was that data protection laws were ineffective in practice, given the ubiquitous, global and networked nature of ICT systems.[23]

Three key insights emerge from the literature of this period. The first is that data protection legislation cannot be effective without the regulation of the actions of all parties involved in the design of ICT systems.[24] This requires that the obligation to implement PbD is

---

[20] For a summary of these measures see Lina Jasmontaite and others, 'Data Protection By Design and by Default: Framing Guiding Principles Into Legal Obligations in the GDPR' (2018) 4 *Eur Data Prot L Rev* 168–189 at 3–5. Article 29 Data Protection Working Party and Working Party on Police and Justice at 2. Also see Peter Hustinx, 'Privacy by Design: Delivering the Promises' (2010) 3 *Identity in the Information Society* 253–255 at 254–255.

[21] European Data Protection Supervisor (EDPS), *Opinion of the European Data Protection Supervisor on the Communication from the Commission to the European Parliament and the Council on the follow-up of the Work Programme for better implementation of the Data Protection Directive* (2007/C 255/01, 2007) at para 2–4. The pragmatism of the EDPS was tempered by a view that 'in the long term changes of the Directive seem unavoidable, while keeping its core principles.' On careful analysis none of those changes were aimed at introducing a new privacy by design principle. On the contrary para 24 states that no new principles are required and the focus of future amendments should be on streamlining the administration of data protection. Para 63 records that policy instruments should be used to address privacy by design.

[22] European Data Protection Supervisor (EDPS), *Opinion of the European Data Protection Supervisor on the communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on 'Radio Frequency Identification (RFID) in Europe: steps towards a policy framework'* (COM(2007) 96 (2008/C 101/01), 2007). The proposed guidelines would set out 'standards' and 'best available techniques' for implementing PbD (para 42, 51-53).

[23] Article 29 Data Protection Working Party and Working Party on Police and Justice.

[24] Hustinx states 'Finally, it would be important to include the principle of "Privacy by Design" among the basic principles of data protection, *and to extend its scope to other relevant parties, such as producers and developers of ICT products and services*. This would be innovative and require some further thinking, but it would be appropriate and only draw the logical consequences of a promising concept' (own emphasis). Although the author's view that PbD must be included as a basic principle of data protection is contrary to the argument made in this chapter, the real impediment to the effective implementation of a PbD approach is, it is submitted, the absence of legislative provisions addressing the legal accountability of other parties in the data eco-system. See also European Data Protection Supervisor (EDPS), *Opinion of the European Data Protection Supervisor on the Communication from the Commission to the European Parliament and the Council on the follow-up of the Work Programme for better implementation of the Data Protection Directive* which states at para 11:
'analysis of the past confirms that improvements cannot be achieved without the involvement of a broad range of stakeholders. The Commission, data protection authorities and the Member States are central actors in most of the actions conducted. However, the role of private parties has an increasing importance, especially when it

not limited to data controllers,[25] but is *extended to parties responsible at an earlier stage* for the setting of standards and the design of the system architecture.[26]

The second was that over-arching legislation must remain technologically neutral, and those general principles in many instances can be implemented (and hence effectively enforced) only through concrete, sector-specific standards and methodologies.[27] The existing legal framework permitted the development of such sector-specific laws but had not been used.[28] Moreover, self-regulation and the adoption by industry of the normative principles of PbD remains essential,[29] but voluntary self-regulation measures alone are insufficient to achieve uniform adoption of a PbD approach.[30]

The third is that requiring privacy as a 'default setting' would significantly enhance privacy protections.[31] The existing legislation promoted a PbD approach, but the creation of a clear legal obligation that privacy must be engineered as the default setting could heighten awareness of consumers and compliance by data controllers, and enable regulators to enforce the measure rather than relying only on 'soft' regulatory measures such as best practice

---

comes to the promotion of self-regulation and European Codes of Conducts, or to the development of Privacy Enhancing Technologies.' See also European Data Protection Supervisor (EDPS), *Opinion of the European Data Protection Supervisor on the communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on 'Radio Frequency Identification (RFID) in Europe: steps towards a policy framework'* at para 55: 'the privacy-by-design principle needs to be introduced at the earliest stage of the development of technologies'. Also see European Data Protection Supervisor (EDPS), *Opinion of the European Data Protection Supervisor on Promoting Trust in the Information Society by Fostering Data Protection and Privacy* at para 33: '[Discussing directive 95/46/EC] They do not explicitly require that information and communications technologies are privacy and data protection compliant, which requires also addressing designers and manufacturers of ICT, including the activities carried out at the stage of standardization.'

[25] Article 29 Data Protection Working Party and Working Party on Police and Justice at 3 and 13.

[26] European Data Protection Supervisor (EDPS), *Opinion of the European Data Protection Supervisor on Promoting Trust in the Information Society by Fostering Data Protection and Privacy* at 8.

[27] Ibid.

[28] Ibid at 9.

[29] A Cavoukian, 'Privacy by Design The 7 Foundational Principles' (2009 (revised January 2011)) <https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf> accessed 26 September 2019. The author states 'Privacy by Design advances the view that the future of privacy cannot be assured solely by compliance with regulatory frameworks; rather, privacy assurance must ideally become an organization's default mode of operation.' By implication aspects of privacy by design cannot be achieved by statutory regulation, but require 'soft' regulatory approaches such as education, advocacy, guidance and industry self-regulation through codes of conduct to encourage the adoption of an approach that goes beyond the minimum threshold set by the legislation.

[30] European Data Protection Supervisor (EDPS), *Opinion of the European Data Protection Supervisor on the communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on 'Radio Frequency Identification (RFID) in Europe: steps towards a policy framework'* para 56.

[31] Article 29 Data Protection Working Party and Working Party on Police and Justice at 13. Also see Tamò-Larrieux who identifies this as the third change brought about by art 25.

guidelines.[32] The view developed that an explicit legal obligation to implement PbD must be included in data protection laws. In 2009, adopting the mantle of 'innovation', the Article 29 Working Party called for the inclusion of both 'PbD' and 'accountability' as 'additional principles' in the data protection legal framework.[33] The argument advanced for including an express obligation to implement PbD as a 'general principle' was acknowledged as an 'extension' of the current rules on technical and organisational measures and closely related to the principle of accountability.[34]

In 2010 the incumbent European Data Protection Supervisor,[35] Peter Hustinx, issued an opinion that to compel compliance with PbD, the concept needed to be incorporated into the data-protection legal framework by way of a 'general, binding principle', coupled with detailed measures to address the particular risks posed by specific technologies.[36] He pointed to existing legal provisions as encompassing PbD in an 'indirect' and 'generic' way. Further, while the legislation provided measures to promote its adoption, it fell short of measures to enforce compliance with a directly stated legal obligation to build privacy into the design of products and to ensure that privacy was protected as the default setting.[37] It was a view that built upon similar views expressed earlier by the Article 29 Working Party,[38] the Information Commissioner's Office in the United Kingdom[39] and the Member of the European Commission

[32] Article 29 Data Protection Working Party and Working Party on Police and Justice. Also see Tamò-Larrieux; and European Data Protection Supervisor (EDPS), *Opinion of the European Data Protection Supervisor on Promoting Trust in the Information Society by Fostering Data Protection and Privacy*.
[33] Article 29 Data Protection Working Party and Working Party on Police and Justice at 2–3.
[34] European Commission, *Safeguarding Privacy in a Connected World. A European Data Protection Framework for the 21st century* (COM(2012) 9 final, 2012) at 7.
[35] The European Data Protection Supervisor (EDPS) is an independent functionary formed in 2001 and carries out supervision of and advice in relation to all Union institutions and bodies, See Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (Text with EEA relevance.) PE/31/2018/REV/1. OJ L 295, 21.11.2018.
[36] European Data Protection Supervisor (EDPS), *Opinion of the European Data Protection Supervisor on Promoting Trust in the Information Society by Fostering Data Protection and Privacy* . The opinion focussed on radio-frequency identification (RFID), social network applications, and browser applications. Also see Hustinx.
[37] European Data Protection Supervisor (EDPS), *Opinion of the European Data Protection Supervisor on Promoting Trust in the Information Society by Fostering Data Protection and Privacy* at 31–37, and particularly para 36.
[38] Article 29 Data Protection Working Party and Working Party on Police and Justice.
[39] Information Commissioner's Office (UK), *Privacy by Design* (2008).

responsible for Information Society and Media in a speech addressing the proposed data protection reforms.[40]

The 2010 Resolution on PbD adopted at the 32nd International Conference of Data Protection and Privacy Commissioners,[41] while stopping short of calling for the adoption of PbD as an additional data protection principle, recognised it as 'an essential component of fundamental privacy protection', and called upon privacy commissioners to 'foster the incorporation of the PbD Foundational Principles in the formulation of privacy policy and legislation within their respective jurisdictions', along with educational and advocacy measures.

In a 2011 paper, Cavoukian emphasised that just as organisations needed to adopt PbD practices, regulators needed to 'innovate', arguing that 'enshrining PbD in regulatory instruments, voluntary codes, and best practices requires an evolution in how policy and law makers approach privacy rule-making'.[42]

IV ARTICLE 25 OF GDPR

Article 25 of GDPR now makes explicit reference to data protection by design and by default.[43]

> *'Article 25*
>
> *Data protection by design and by default*
>
> 1. *Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective*

[40] Viviane Reding, 'Privacy: the Challenges Ahead for the European Union; Keynote Speech at the Data Protection Day' (*European Parliament*, 28 January 2010) <https://europa.eu/rapid/press-release_SPEECH-10-16_en.htm> accessed 28 September 2019.
[41] *Resolution on Privacy by Design* (Jerusalem, 29 October 2010).
[42] A Cavoukian, *Privacy by Design in Law, Policy and Practice A White Paper for Regulators, Decision-makers and Policy-makers* (Information and Privacy Commissioner, Ontario, Canada, 2011) at 3.
[43] GDPR art 25.

manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.

2. *The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.*

3. *An approved certification mechanism pursuant to Article 42 may be used as an element to demonstrate compliance with the requirements set out in paragraphs 1 and 2 of this Article.'*

What is immediately apparent from the text of article 25 is that it does not introduce any additional core data protection principle or data subject right. On the contrary, article 25(1) explicitly states that the PbD approach requires the implementation of measures 'designed to implement data-protection principles … in an *effective manner*' (own emphasis). This is consistent with the conceptualisation of PbD as being not only a philosophy underpinning data protection, but also a methodology for the *effective implementation* of data protection principles.[44]

Article 25(1) explicitly requires that such measures be implemented not during processing but from the earliest stage, when the means of processing is first determined. The definition of processing extends from collection through to erasure or destruction.[45] The phrase 'means of processing' is a broad one encompassing both 'abstract' and 'concrete' elements of the technology design.[46] Likewise the 'determination' of the means refers broadly to the

[44] A Cavoukian, 'Privacy by Design The 7 Foundational Principles Implementation and Mapping of Fair Information Practices' <https://iab.org/wp-content/IAB-uploads/2011/03/fred_carter.pdf> accessed 17 September 2019.

[45] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA OJ L 119, 4.5.2016 (EU General Data Protection Regulation; GDPR) art 4(2).

[46] European Data Protection Board (EDPB), *Guidelines 4/2019 on Article 25 Data Protection by Design and by Default* (13 November 2019) at 10. The guidelines list 'the architecture, procedures, protocols, layout and appearance' as part of the means of processing.

'process' of deciding which means to use, and not simply to the point at which a final decision is made.[47] Thus, article 25(1) is consistent with the 'cradle-to-grave' data privacy concept set out in the PbD foundational principles, but it is given legal effect through the accountability provision, which requires the data controller to demonstrate compliance with all data-protection principles.[48]

Article 25(2) explicitly provides that by default, only personal data which are necessary for each specific purpose of the processing are processed. The core data protection principle of data minimisation requires that data processing must be limited to such personal data as is necessary for the specific purpose, and article 25(2) does not go beyond this.[49] While article 25(2) is undeniably important insofar as it makes it clear that default settings[50] must comply with GDPR,[51] arguably, this was always implied by the requirement of opt-in consent for specific purposes that go beyond what is strictly necessary for the service, required by law, or within the legitimate interests of the data controller.

V CRITIQUE OF ARTICLE 25

By including article 25, GDPR has signalled that PbD is not simply a best practice recommendation but 'a legal and full enforceable obligation that all those who process personal data under EU law must comply with'. [52] In theory, a failure to implement PbD is a breach of

[47] Ibid.
[48] Ibid art 5(2). Unlike section 8 of POPIA the article does not contain the additional proviso that compliance must be effected both during processing and earlier, when the purpose and means of processing is determined. However this is clear when art 5(2) is read together with art 25(1).
[49] It does not require a restriction of collection to a 'strict minimum'. Processing that is strictly necessary for the service, or required by the legitimate interests of the data controller (such as internal processes related to the provision of the service and security and fraud detection measures) are lawful without consent. Consent therefore is possible (and in fact only required) when the purpose of processing requires the collection of personal information that goes beyond what is strictly necessary.
[50] EDPB at 10 refers to default settings as 'any pre-existing or preselected value of a configurable setting that is assigned to a software application, computer program or device.'
[51] Lee A Bygrave, 'Data Protection by Design and by Default: Deciphering the EU's Legislative Requirements' (2017) 4 *Oslo Law Review* 105–120. The author states: 'The duty builds on and elaborates the more generally formulated provisions on 'responsibility of the controller' in Article 24. It is formulated in very similar terms to the duty to ensure adequate security of processing under GDPR Article 32. Yet, unlike the latter, the duty under Article 25 extends to ensuring – apparently without qualification – default application of particular data protection principles and default limits on data accessibility.'
[52] European Data Protection Supervisor (EDPS), *Opinion 5/2018 Preliminary Opinion on Privacy by Design* (2018) at 8.

GDPR, raising the possibility of enforcement measures.[53] The sanction of large fines [54] may be the first real 'economic incentive' to spur the adoption of a PbD approach,[55] as the implementation of PbD is a factor which will weigh in the assessment of the amount of any fine.[56] In addition, an explicit PbD right clearly signals to industry that enforcement authorities require its de facto application in practice[57] and that it should be integrated into information and communication systems and solutions.[58]

However, one should be cautious not to overstate the impact of article 25. The inclusion of article 25 is a 'conversation-starter',[59] but without detailed guidance by data supervisory authorities on what steps are required to implement a PbD approach in specific contexts, it is difficult to envisage how the article will be enforced.[60] Critics have indicated that 'data controllers have little clue how they should go about "designing in" privacy'.[61]

The concept of PbD is not defined in the legislation,[62] and has been criticised as vague.[63] On the one hand it may require no more than the 'relatively straightforward' adoption of privacy-enhancing technologies such as encryption and role-based access controls,[64] which

---

[53] GDPR art 58(2) includes measures such as warnings, reprimands, orders to comply and limitations or bans on processing.
[54] GDPR art 83(4)(a) provides that an administrative fine of up to €10 million, or in the case of an undertaking up to 2% of the total worldwide annual turnover of the preceding financial year, whichever is higher.
[55] Jeroen van Rest and others, 'Designing Privacy-by-Design' [2014] *Privacy Technologies and Policy* 55 at 57.
[56] GDPR art 83(2)(d) requires that 'due regard' be paid to the implementation of technical and organisational measures under art 25 and 32 to determine the degree of responsibility of any controller or processor that has breached the Regulation.
[57] European Data Protection Supervisor (EDPS), *Opinion of the European Data Protection Supervisor on Promoting Trust in the Information Society by Fostering Data Protection and Privacy* at 8.
[58] Ibid.
[59] Bygrave at 120. The author frames his paper within the broader scholarship on the effectiveness of regulatory 'conversations' begun by Julia Black, 'Regulatory Conversations' (2002) 29 *Journal of Law and Society* 163–196. Two aspects of this discourse are particularly apposite to the present study on mobile applications: the difficulty of translating legal concepts into concrete IS systems goals and steps that developers understand, and the power dynamics between parties in the apps eco-system which make it difficult for developers to implement privacy by design even if they wanted to. See further Chris Reed, 'You talkin' to me?' in Dag Wiese Schartum, Lee A. Bygrave and Anne Gunn Berge Bekken (eds), *Jon Bing: En Hyllest / A Tribute* (Gyldendal Akademisk 2014).
[60] European Data Protection Supervisor (EDPS), *Opinion 5/2018 Preliminary Opinion on Privacy by Design* , noting that data protection supervisory authorities will have to provide such guidance.
[61] Bert-Jaap Koops and Ronald Leenes 'Privacy Regulation Cannot Be Hardcoded: A Critical Comment on the 'Privacy by Design' Provision in Data Protection Law' (2014) 28 (2) *International Review of Law, Computers & Technology* 159–171 at 160.
[62] Ibid.
[63] van Rest and others at 56 *et seq*. The author is commenting on the original Commission proposal for reform, but the final text of GDPR also does not define Privacy by Design, although it remains the case that a range of soft regulatory instruments are available to concretise the concept in particular application contexts.
[64] Koops and Leenes at 160.

arguably go no further than existing conditions for security and accountability. On the other hand, if it requires privacy to be 'hardcoded' into technology products, by developing 'machine-executable code' that automatically implements privacy-preserving outcomes,[65] it may be unattainable, and even counterproductive.[66] The likelihood is that without further detailed, sector-specific guidance, companies will continue to implement the concept in different ways, creating additional complexity rather than the desired transparency.[67] At the same time, overly prescriptive regulatory measures may stifle innovation.

The inclusion of article 25 should thus not detract from the continued necessity to develop detailed guidance through 'soft' regulatory measures, such as education, industry consultation and approved codes of conduct which reference applicable approved industry standards and methodologies, in order to 'translate' the legal requirements into practical steps for implementation in a particular sector.

The absence of an explicit statutory requirement for PbD is not an impediment to the development of regulatory measures to promote the adoption of the concept. In the US a PbD approach has been incorporated into the policy framework for consumer privacy protection, and has advanced through the terms of settlements reached in FTC enforcement actions under sectoral privacy laws.[68] Likewise, in Europe, case law in the European Court of Human Rights and in the Court of Justice of the European Union (CJEU) reflects the application of PbD ideals.[69]

---

[65] Ibid.
[66] Ibid at 167. The authors explain that including code to verify privacy compliance may entail collecting more personal information than is necessary for the system to function.
[67] Ibid.
[68] Bygrave at 107.
[69] Ibid at 109. The author discusses *I v Finland* no 20511/03, ECHR 2008 arguing that implicitly the court applied a privacy by design approach that went beyond extant data protection requires (de jure protections) but is compatible with GDPR art 25(2). While health data is quintessentially *private* information the author argues that the same approach should be followed in relation to other sensitive personal information, and to all personal information when the context requires, such as when unfair discrimination might result from any processing (i.e. the approach should not be restricted to confidentiality requirements implicated by unlawful disclosure of private information). Indirectly the author argues that the aims of privacy by design were also addressed by the CJEU in *Scarlet Extended v Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)* (C-70/10) ECLI:EU:C:2011:771; *SABAM v Netlog* (C-360/10) ECLI:EU:C:2012:85; *Google Spain SL and Google Inc* (C-131/12) ECLI:EU:C:2014:317 and *Digital Rights Ireland* (C-293/12 and C-594/12) ECLI:EU:C:2014:238.

VI ACCOUNTABILITY

Some of the most significant changes introduced by GDPR have no direct impact on PbD, namely its extended territorial scope,[70] increased penalties,[71] mandatory breach notification,[72] and the rationalisation of data-protection reporting requirements.[73] As outlined in chapter 5, GDPR has also expanded upon the provisions for consent, security and the rights of the data subject, but in key respects POPIA provides materially similar protections (as set out in chapter 6). What does require further detailed discussion is the introduction of 'accountability'.

The 1995 Data Protection Directive did not contain an express accountability principle,[74] whereas GDPR and POPIA do. This is an important provision in relation to a PbD approach.[75] It is not, however, a new data-protection principle.[76] The principle of accountability was contained in the Organisation for Economic Co-operation and Development (OECD) Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal

---

[70] GDPR applies to all companies processing the personal data of data subjects residing in the European Union (even where the processing takes place outside the European Union). This removes the ambiguity created by the reference to processing 'in context of an establishment' in the European Union created by the 1995 Directive. Under GDPR if a controller or processor is not based in the European Union but their activities involve offering goods or services to EU citizens (including free goods and services) or monitoring behaviour that takes place within the EU, they will be bound by GDPR and must appoint a representative in the EU.

[71] For serious infringements, which includes processing data without adequate user consent, or in violation of core privacy principles, organisations can be fined up to 4% of annual global turnover or €20 Million. These fines apply to controllers and processors, and are significantly higher than the penalties prescribed under the 1995 Directive, or under POPI.

[72] In all EU member states there is now a mandatory requirement that data controllers give notice of a data breach that is likely to 'result in a risk for the rights and freedoms of individuals' within 72 hours of becoming aware of the breach. Similarly all data processors must give notice of data breaches 'without undue delay'. These provisions must be read with the requirement to have reasonable and adequate security safeguards to detect data breaches.

[73] GDPR does away with the cumbersome and costly requirements to register data processing activities with, and obtain approval for, contract and data transfer terms from multiple data protection agencies. The approval of third party data transfers and industry self-regulation measures such as model contract clauses and codes of conduct is centralised in the European Data Protection Board. The record-keeping necessary for data protection compliance is handled internally by a Data Protection Officer, who must be duly certified, but it is only mandatory to employ a DPO when a data controller's core activities involve regular and systematic monitoring of data subjects on a large scale or of special categories of data or data relating to criminal convictions and offences.

[74] Data Protection Directive 95/46/EC rec 18 referred to the responsibility of a data controller as follows:
'Whereas, in order to ensure that individuals are not deprived of the protection to which they are entitled under this directive, any processing of personal data in the Community must be carried out in accordance with the law of one of the Member States; whereas, in this connection, processing carried out under the responsibility of a controller who is established in a Member State should be governed by the law of that State.'

[75] Hustinx at 254. Also see European Commission at 7.

[76] OECD, *Thirty Years After the OECD Privacy Guidelines* (2011) at 52–53.

Data.[77] Legal accountability for complying with measures to give effect to the data protection principles set out in the Guidelines rests with the data controller.[78]

The accountability principle was not originally contained in the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (COE Convention 108). However, an accountability principle has been introduced by Article 10(1) of Convention 108, as amended by the 2018 Protocol, which will become effective when the Protocol enters into force.[79] In the Madrid Resolution, the accountability principle was recognised by data protection and privacy commissioners as part of a set of principles that would provide an internationally uniform approach.[80] Accountability was identified by the Article 29 Working Party[81] as a key principle for ensuring that data controllers take a proactive approach to data protection.[82]

The accountability principle does not abrogate or modify any of the other principles of data protection – it enhances their effectiveness, in that it requires data controllers to implement measures to achieve compliance with data protection principles, and to

---

[77] OECD, *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980) (1980) (revised 2013): 'Accountability Principle 14. A data controller should be accountable for complying with measures which give effect to the principles stated above.'

[78] OECD, *Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data* (C(80)58/FINAL, as amended on 11 July 2013 by C(2013)79, 2013) art 14.

[79] Convention for the Protection of Individuals with Regard to the Processing of Personal Data (ETS 108) amended by protocol to the Convention for the Protection of Individuals with Regard to the Processing of Personal Data, adopted by the Committee of Ministers at its 128th Session in Elsinore on 18 May 2018 (CETS 223). This provides:

'Article 10 – Additional obligations

1 Each Party shall provide that controllers and, where applicable, processors, take all appropriate measures to comply with the obligations of this Convention and be able to demonstrate, subject to the domestic legislation adopted in accordance with Article 11, paragraph 3, in particular to the competent supervisory authority provided for in Article 15, that the data processing under their control is in compliance with the provisions of this Convention.'.

[80] Spanish Data Protection Authority, 'Joint Proposal for a Draft of International Standards on the Protection of Privacy with regard to the processing of Personal Data (The Madrid Resolution)' (International Conference of Data Protection and Privacy Commissioners,Madrid, 5 November 2009). The resolution does not call for the introduction of a new "Privacy by Design" principle.

[81] The Working Party was an advisory body established under art 29 of Data Protection Directive 95/46/ECand comprised representatives from the data protection authorities of each EU member state, the EU Commission, and the European Data Protection Supervisor. The Working Party has been replaced by the European Data Protection Board established under art 68 of GDPR.

[82] Article 29 Data Protection Working Party, *Opinion 3/2010 on the Principle of Accountability* (WP173, 13 July 2010) especially the comment at 3 that accountability mechanisms are key for moving data protection 'from "theory to practice"'. Also see similar views expressed earlier in Article 29 Data Protection Working Party and Working Party on Police and Justice.

demonstrate compliance when requested to do so by data protection authorities.[83] Pursuant to these developments, the accountability principle is now expressly included in article 5(2)[84] and article 24[85] of GDPR.

The accountability principle plays a key role in how a PbD approach will be implemented, and must be read together with provisions in GDPR regulating the data controller's responsibility to implement appropriate technical and organisational measures for the lawful processing of personal data,[86] and the obligation to document those measures 'where possible',[87] and with an exemption for certain small and medium-sized enterprises.[88]

First, processing is only lawful where it is carried out for a specified purpose or for a further compatible purpose.[89] The implementation of 'appropriate safeguards' is one of the factors relevant to the assessment of whether further processing of data is compatible with

---

[83] Article 29 Data Protection Working Party, *Opinion 3/2010 on the Principle of Accountability* at 5. The actual measure must vary according to the nature of the data and the risks associated with the processing being carried out.

[84] GDPR art 5(1) sets out the principles of lawful processing: lawfulness, fairness, transparency, purpose limitation, purpose specification, data minimisation, accuracy, storage limitation, and integrity and confidentiality. Art 5(2) provides: *The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability').*

[85] GDPR art. 24 reads:

'Responsibility of the controller

1 Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation.

2 Those measures shall be reviewed and updated where necessary. Where proportionate in relation to processing activities, the measures referred to in paragraph 1 shall include the implementation of appropriate data protection policies by the controller.

3. Adherence to approved codes of conduct as referred to in Article 40 or approved certification mechanisms as referred to in Article 42 may be used as an element by which to demonstrate compliance with the obligations of the controller.'

[86] Bygrave at 116 notes that GDPR fails to make clear how art 25 will impact the application of these provisions.

[87] GDPR art 30(1), in particular 30(1)(f) and (g) which are qualified by the proviso 'where possible'. Also see art 30(2) which places a similar duty on the processor. Both controllers and processors (or their representatives) must make such records available to the supervisory authority of an EU member state 'upon request'.

[88] Ibid art 30(5), which provides:

'The obligations referred to in paragraphs 1 and 2 shall not apply to an enterprise or an organisation employing fewer than 250 persons unless the processing it carries out is likely to result in a risk to the rights and freedoms of data subjects, the processing is not occasional, or the processing includes special categories of data as referred to in Article 9(1) or personal data relating to criminal convictions and offences referred to in Article 10'

[89] Ibid art 5(1)(b). Also see rec 50.

'1. Personal data shall be:

…

b. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ("purpose limitation").'

the original purpose of data collection.[90] It is further a factor in the lawfulness of processing special personal data,[91] data relating to criminal convictions and offences,[92] data that have not been obtained directly from the data subject,[93] data excluded from certain protections under national law,[94] identification numbers,[95] archival, research and statistical data,[96] data protected by a professional or equivalent duty of secrecy,[97] data used for automated profiling,[98] and children's data.[99] Adequate safeguards also inform the data protection impact assessment,[100] adequacy decisions in relation to cross-border data transfers,[101] and international co-operation.[102]

Secondly, although a data controller must document all data breaches,[103] a report to the supervisory authority is not required if 'the personal data breach is unlikely to result in

---

[90] Ibid art 6(4)(e). Pseudonimisation and encryption are provided as examples included within the meaning of the term 'appropriate safeguards'. The provision impliedly refers to the controller's duties under art 25 and art 32.
[91] Ibid art 9. E.g. health data.
[92] Ibid art 10.
[93] Ibid art 14, especially 14(5)(b) which relaxes the requirement for informing the data subject where it would be 'impossible or would involve disproportionate effort' to do so, or would render impossible or seriously impair the objectives of processing; subject to 'appropriate measures to protect the data subject's rights and freedoms and legitimate interests, including making the information publicly available'.
[94] Ibid art 23. E.g. on the grounds of national security.
[95] Ibid art 87. Such processing may be further regulated by national law.
[96] Ibid art 89 records that such 'safeguards shall ensure that technical and organisational measures are in place in order to ensure in particular respect for the principle of data minimisation.' Where possible such processing 'shall' be fulfilled in a manner that 'does not permit or no longer permits the identification of data subjects.' Rec 156 refers to the 'proportionality and necessity principles'.
[97] Ibid art 90.
[98] Ibid art 22(3) requires the implementation of 'suitable measures' to safeguard the data subject's rights.
[99] Ibid rec 38 records that children merit 'special protection', although GDPR does not outline any additional safeguards beyond parental consent for the processing of children's data contained in art 8. The 1995 data protection directive contained no specific provisions concerning children's data.
[100] Ibid art 35. The requirement pertains only to 'high risk' processing. High risk processing comprises automated profiling or large scale processing of sensitive data or large scale monitoring as set out in art 35(3). In terms of art 35(4) or (5) the supervisory authority can publish a list of processing activities determined to be high risk and those exonerating from the requirement of an impact assessment. When an impact assessment is warranted and reveals a high risk to the rights and freedoms of natural persons in absence of mitigating measures the supervisory authority must be consulted in terms of art 36 prior to the processing being carried out.
The requirements for an impact assessment are set out in art 35(7):
'The assessment shall contain at least: a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller;
an assessment of the necessity and proportionality of the processing operations in relation to the purposes;
an assessment of the risks to the rights and freedoms of data subjects referred to in paragraph 1;
and the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned.'
[101] Ibid chapter V, especially art 46, 47 and 49(1), read with article 14(1)(f) and 15(2).
[102] Ibid art 50.
[103] Ibid art 33(5).

a risk to the rights and freedoms of natural persons'.[104] For example, the right to privacy is at risk if the breach included data in a personally identifiable form. The section does not explicitly indicate how this provision will be read with articles 25 and 32.[105] Clearly the extent of the technical and organisational safeguards in place must be taken into consideration in determining the risks posed by a data breach, but whether measures such as pseudonymisation and encryption of data mean that there is no risk must be determined on a case-by-case basis. This is made clearer when article 33 is read with the requirement that where there is a '*high* risk' (own emphasis), the data breach must be reported to the data subject(s) affected by the breach,[106] unless 'appropriate technical and organisational protection measures' have been applied to the personal data, 'such as encryption'.[107]

Last, the extent of the controller's responsibility is determined with reference to the 'technical and organisational measures' implemented by the controller when a supervisory authority decides whether to impose a fine (and the amount of such fine) for breach of GDPR.[108] While there is little additional guidance in GDPR itself on what such technical and organisational measures entail, GDPR encourages pseudonymisation,[109] and provides some

[104] Ibid art 33(1).
[105] Bygrave at 116.
[106] GDPR art 34(1).
[107] Ibid art 34(3)(a).
[108] Ibid art 83(2)(d) refers to 'technical and organisational measures' taken pursuant to both art 25 and art 32. However as Bygrave notes, art 25 is worded in 'very similar' terms to art 32, but with the additional requirement that these measures be default settings.
[109] Ibid rec 29.

stipulations for automated processing,[110] internal policies to address data protection by design[111] and considerations for the appointment of processors.[112]

VII THE ACCOUNTABILITY GAP

The introduction of a PbD 'principle' was discussed against the backdrop of requiring PbD in the architecture of ICT systems,[113] and if the insights of Pb(re)D had been applied the drafters of GDPR might have taken measures to ensure that the redesign of existing technologies and systems was implemented through the assignment of clear legal duties on all roleplayers. The amendments to GDPR have failed to address this shortcoming.[114] In its final version, article 25 was restricted in application to data controllers,[115] who must control the 'downstream' application of PbD by processors through contractual means.[116] As set out in chapter 5, the data

---

[110] Ibid rec 71. While retaining the reference to 'appropriate' technical and organisational measures, the recital flags four areas that must be addressed by such measures: correction of inaccuracies, minimisation of the risk of error, security and prevention of discriminatory effects (in relation to race or ethnic origin, political and religious beliefs, trade union membership, genetic or health status and sexual orientation).

[111] Ibid rec 78.

While retaining general reference to 'appropriate technical and organisational measures' the recital further states that '[i]n order to be able to demonstrate compliance with this Regulation, the controller should adopt internal policies and implement measures which meet in particular the principles of data protection by design and data protection by default. Such measures could consist, inter alia, of minimising the processing of personal data, pseudonymising personal data as soon as possible, transparency with regard to the functions and processing of personal data, enabling the data subject to monitor the data processing, enabling the controller to create and improve security features. …'.

Nothing of substance is added to the legal obligations: data minimisation, transparency, data subject participation and security are existing legal principles that must be complied with to demonstrate lawful processing. Pseudonymisation is one measure that may be used, and is 'encouraged' (rec 29) but as technology advances at an unprecedented pace, the appropriateness of the measures taken must be assessed on a case by case basis.

[112] Ibid rec 81, records that the 'sufficient guarantees' required of a processor must be 'in particular in terms of expert knowledge, reliability and resources'.

[113] Article 29 Data Protection Working Party and Working Party on Police and Justice at 3 states: 'privacy and data protection should be integrated into the design of Information and Communication Technologies. The application of such principle would emphasize the need to implement privacy enhancing technologies, 'privacy by default' settings and the necessary tools to enable users to better protect their personal data. *This principle of 'Privacy by Design' should therefore not only be binding for data controllers, but also for technology designers and producers*. On top of that, as the need arises, regulations for specific technological contexts should be adopted which require embedding data protection and privacy principles into such contexts.' (own emphasis). Also see Hustinx.

[114] Accountability rests solely with the data controller. Whilst there may be more than one data controller, and sub-processors, the legislation has not addressed the legal accountability of software and hardware manufacturers and platform providers who may not directly process data, but who may exercise considerable influence over the extent to which privacy is (and can be) embedded into the design of IT systems. Nor has it addressed the 'blurry' line between controllers, processors and data subjects that arises in the context of a networked cloud-computing environment. See Article 29 Data Protection Working Party and Working Party on Police and Justice at 12.

[115] Bygrave at 109 notes that the European parliament had put forward a draft which extended art 25 to processors.

[116] Ibid at 116. Also see GDPR art 28(1). For discussion of the deliberations see Jasmontaite and others at 171-172. Both Bygrave (at 116-117) and Jasmontaite and others (at 171) note that the final text neither makes PbD directly applicable to processors, nor is it a prerequisite for public tenders.

'controller' can appoint one or more 'processors' in terms of a contract, but can also disclose personal information to a 'third party'. There can be 'joint controllers', and a third party who will process the personal information could be regarded as a data controller.

A key issue that is not addressed in GDPR or the supervisory guidelines is how accountability is assigned when there are multiple controllers. For example, in Belgium, 'large-scale processing of personal data whereby the behavior [*sic*] of natural persons is systematically observed, collected, established or influenced by automated processing, including for advertising purposes' is viewed as 'high risk'.[117] Behaviour includes '[f]or example viewing, listening, browsing, clicking, physical or purchasing behaviour'.[118] The guidance indicates that '[t]he controller who *envisages* one of the aforementioned types of processing is obliged to carry out a DPIA prior to the processing' (own emphasis).[119] The ad network, the advertiser and the publisher (in the case of a mobile app, the developer who integrates an ad library to monetise the app through advertising) would 'envisage' that data about which ads are viewed or clicked on will be collected for attribution of ad revenue. Additionally, they would envisage that other personal information, including location, could be collected for targeted advertising. The app developer does not have insight into how the ad network processes the data, but insofar as he or she agrees to participate in advertising, the app developer may be said to determine both the means and purpose of processing. As such, the app developer is a controller in respect of 'high risk' processing, and a DPIA would appear to be mandatory.

By contrast, in the United Kingdom, 'online advertising' is included as 'high risk' where the personal data is not obtained directly from the data subject and the controller, and relying on article 14(5)(b) does not give notice to the data subject.[120] This could exclude the vast majority of in-app advertising, using the argument that by virtue of the code in the ad library, the information is transmitted from the user's device *directly* to the ad network. It is thus not obtained from a third party. In any event, if the app developer has obtained consent for the purpose of advertising, then this would appear to exclude such advertising from consideration as 'high risk'.

---

[117] Data Protection Authority (Belgium), *List of the Types of Processing Operations for which a DPIA shall be Required (Section 35 (4) of the GDPR)* (2019).
[118] Ibid.
[119] Ibid. They must then assess if the risk can be adequately reduced by appropriate technical and organizational measures, and if so, may not need a prior consultation with the supervisory authority.
[120] Information Commissioner's Office (UK), *Examples of Processing "Likely to Result in High Risk"* (2019).

Last, in Iceland, advertising is not specifically mentioned, but the somewhat broader categories of service delivery and product development is implicated as high risk where, inter alia, it is based on the prediction of preferences, interests, behaviour or location, even if this does not take place on a 'large scale'.[121] This could thus include all targeted (interest-based) advertising, but may also include app analytics providing the app developer with statistics on audience segments and conversion events.

In all of these instances, it is unclear how a DPIA by the mobile app developer can be properly undertaken without transparent information from third parties about how data will be further processed. Given the imbalance in power between very large platforms and small app developers, it seems unlikely that they have the contractual 'muscle' to enforce transparency. Some suggest that SMMEs may simply ignore privacy requirements, or may be disincentivised to develop new technologies if the legal obligations are insufficiently clear and the risks of liability are too great.[122]

The more effective solution would be to require large platforms that are processing personal information, such as analytics providers, social network platforms, ad networks and ad exchanges, to conduct mandatory DPIAs and consult with the supervisory authorities before undertaking processing.

The 'upstream' application of PbD is not directly regulated.[123] Recital 81[124] appears to envisage that data controllers will pass their obligation on to technology

---

[121] Icelandic Data Protection Authority, *Notice on Processing Operations Subject to the Requirement of a Data Protection Impact Assessment* (2019) includes on its DPIA list '[p]rocessing personal data with the purpose of providing services or developing products for commercial use that involve predicting working capacity, economic status, health, personal preferences or interests, trustworthiness, behaviour, location or route in conjunction with at least one other criterion (Sensitive data or data of highly personal nature and evaluation/scoring).' The list does not specify that this must be on a 'large scale'.

[122] Laurence Diver and Burkhard Schafer 'Opening the Black Box: Petri Nets and Privacy by Design' (2017) 31 (1) *International Review of Law, Computers & Technology* 68–90 at 71–72. The author also warns that conversely larger platforms may make 'token' gestures towards a PbD approach without implementing real change.

[123] Bygrave at 116. Also see Giorgia Bincoletto, 'A Data Protection by Design Model for Privacy Management in Electronic Health Records' in *Annual Privacy Forum: Privacy Technologies and Policy* (Springer, Rome, Italy 13–14 June 2019) at 169 and European Data Protection Supervisor (EDPS), *Opinion 5/2018 Preliminary Opinion on Privacy by Design* at 8. The 'design phase' may begin long before a controller assumes that role, with the producers, programmers and developers of hardware and software systems that will be employed for processing.

[124] GDPR rec 81. The relevant portion reads:

'When developing, designing, selecting and using applications, services and products that are based on the processing of personal data or process personal data to fulfil their task, producers of the products, services and applications should be encouraged to take into account the right to data protection when developing and designing such products, services and applications and, with due regard to the state of the art, to make sure that controllers and processors are able to fulfil their data protection obligations.'

developers.[125] However, as it provides only that the producers of products, services and applications are 'to be encouraged to take into account the right to data protection', it is not only less onerous than article 25, but also not in any way a directly enforceable legal obligation.[126] The amendment of the e-Privacy Directive poses an opportunity to create such an extended legal obligation, but the current draft does not contain any provisions to this effect.[127]

In a mobile apps setting, widespread industry change is likely to happen only if app stores actively enforce their review guidelines by not listing mobile apps that do not comply with data protection legislation and if device manufacturers and OS platforms address the shortcomings of the small screen and current permission architecture to make it necessary (and easy) for developers to provide clear notice about the purpose of requesting information, and to provide granular opt-in consent for such different purposes. For example, apps already require user-granted run-time permission to access location information and notify the user that location is being collected through an icon displayed on the user interface. However, permission requests do not allow users to block sharing of location with third parties at an OS level. Location services can either be turned on (thus permitting all purposes of processing location) or be turned off completely (which, as explained in chapter 2, still does not necessarily prevent the collection of location through other means). It is submitted that without adequate

---

[125] Bygrave at 116.

[126] Yordanka Ivanova, 'Data Controller, Processor or a Joint Controller: Towards Reaching GDPR Compliance in the Data and Technology Driven World' (Forthcoming) in Tzanou M (ed), *Personal Data Protection and Legal Developments in the European Union* (IGI Global, 2020), < https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3584207> accessed 10 August 2020 at 15 and 18. Ivanova argues that to achieve data protection by design and by default technology providers (by which she refers to 'developers and manufacturers of software and other data processing technlogies' whether they be products or services) must be held accountable as 'fully fledged joint controllers', but accepts that it is 'unclear' to what extent GDPR art 25 applies to them.

[127] European Data Protection Supervisor (EDPS), *Opinion 5/2018 Preliminary Opinion on Privacy by Design* at 9. Also see European Data Protection Supervisor (EDPS), *Opinion on the Proposal for a Regulation on Privacy and Electronic Communications (ePrivacy Regulation)* (2017) at 18–19 decrying the fact that the proposal for an e-Privacy Regulation does not include an explicit reference to the requirement that consent be configured using *default* privacy settings the EDPS called for inclusion of an obligation 'on hardware and software providers to implement default settings that protect end users' devices against any unauthorised access to or storage of information on their devices.' The EDPS was commenting on art 9 and 10 of the original draft, which have proved particularly contentious. The legislative process is ongoing. See: Proposal for a regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) Brussels, 10.1.2017 COM(2017) 10 final 2017/0003 (COD).

measures to enforce accountability of all parties in the mobile applications ecosystem, a PbD provision in legislation may create illusory rather than real-world data protection.

VIII CONCLUSION

In summary, while there may be some advantages to including a PbD obligation explicitly in legislation, those advantages should not be overstated and the particular reasons why the EU favoured including an explicit PbD article to overcome the complexities of the EU legal system should not be overlooked.

Article 25 should furthermore be evaluated against the three key issues identified in the literature. First, without accountability of all role-players, PbD cannot be fully realised. A fortiori Pb(re)D in relation to complex multi-party, multi-layer data processing operations, such as one encounters in the mobile apps ecosystem will be all but impossible to enforce through legal means. Article 25 does not address this issue adequately as it does nto impose clear legal duties on all roleplayers. Second, legislation must remain technologically neutral. Article 25 does this, retaining the 1995 Directive reference to ‘adequate technical and organisational measures’ without exhaustively addressing such measures. Third, PbD requires that privacy be a default setting. However, as it stands, article 25(2) is too vague to be effectively enforced without the development of detailed standards, and methodologies for the implementation of PbD and the configuration of default settings in a particular context.

CHAPTER 9

A "PRIVACY BY DESIGN" APPROACH UNDER THE PROTECTION OF PERSONAL INFORMATION ACT

I INTRODUCTION

This chapter builds on the earlier chapters to offer an analysis of whether, despite the absence of an express provision similar to article 25 of GDPR, a Privacy by Design (PbD) approach is nevertheless implied under POPIA. The discussion of the application of PbD in South Africa includes the f of Privacy by (re)Design, which is underpinned by the same foundational principles but seeks to move beyond their application in the design of new technologies, practices and systems, to achieve the *redesign* of existing technologies and systems.

The chapter begins with an argument for implied obligations under a statute. It then sets out the powers and functions of the Information Regulator in South African and identifies the development of a PbD guideline for mobile app developers in South Africa as the necessary first step for developing a regulatory 'conversation' around the implementation of PbD in the mobile apps ecosystem in South Africa. The chapter then analyses the relevant statutory provisions in POPIA and the extent to which they align with PbD, as the foundation for such a guide.

II A PbD APPROACH IMPLIED BY LEGISLATION

The introduction of article 25 in the European context must be understood in the light of the complex European legal system. The primary driver for data protection reform in Europe was the fact that the 1995 Data Protection Directive had not been uniformly implemented in national law, and it had long been regarded as inevitable that legal reform was needed to simplify and unify the administration of data protection law within the Union.[1] GDPR is a

[1] European Data Protection Supervisor (EDPS), *Opinion of the European Data Protection Supervisor on the Communication from the Commission to the European Parliament and the Council on the follow-up of the Work Programme for better implementation of the Data Protection Directive* (2007/C 255/01, 2007) para 24. The report is clear that in EDPS does not regard it as necessary to introduce new principles, and that greater effectiveness, inter alia, in promoting Privacy by Design, can be achieved policy measures. This view was later modified and the EDPS supported the introduction of the accountability principle and an express PbD article, proposed by the WP29.

Regulation which had immediate effect as law in all member states from 25 May 2018.[2] It has reduced the possibilities for inconsistent application of data protection principles, by data supervisory authorities, courts and legislatures in each member state.[3]

An understanding that the European codified legal system favours direct and detailed legislative prescripts of concepts that may underpin and inform the interpretation of wider, principles-based legislation in countries with a common law heritage or a hybrid legal tradition, such as South Africa, is essential. It would be wholly incorrect to assume that because POPIA does not explicitly refer to PbD, such an approach is not required for compliance with its provisions. On the contrary, an obligation may be implied by a South African statute, and thus PbD is capable of being articulated through the interpretation and application of the guiding principles in particular contexts by the Information Regulator, the judiciary, and organisations processing personal information, and role-players in the wider mobile apps ecosystem.

III A RANGE OF REGULATORY ENFORCEMENT MEASURES

The Information Regulator is empowered to exercise a range of regulatory enforcement measures. These are set out briefly here, and their application is considered further below where relevant;[4]

1. Grant exemptions for certain processing, such as statistical activities, subject to reasonable conditions;[5]

---

[2] Jeroen van Rest and others, 'Designing Privacy-by-Design' [2014] *Privacy Technologies and Policy* 55 at 61. GDPR does permit derogations by way of national law on certain matters and will be enforced by a national supervisory authority in each member state. The creation of the European Data Protection Board is however intended to serve a unifying function, to harmonise the interpretation and application of GDPR.

[3] See as to the difficulties of achieving harmonisation under Directive 95/46/EC: *Lindqvist* (C-101/01) ECLI:EU:C:2003:596 para 96, *Huber* (C-524/06) ECLI:EU:C:2008:724 para 50, *Asociación Nacional de Establecimientos Financieros de Crédito* (C-468/10 and C-469/10) ECLI:EU:C:2011:777 para 28–32, *IPI* (C-473/12) ECLI:EU:C:2013:715 para 31 and *Breyer* (C-582/14) ECLI:EU:C:2016:779 para 57.

[4] As a general principle 'smart' regulatory approaches adopt a range of complementary and overlapping measures. See on the 'smart' regulatory approach Heath William Evans, 'Corporate social responsibility (CSR): tailoring regulation and government policy to the needs of small and medium-sized enterprises' (2017). It is to be hoped that the Information Regulator will make use of the full range of its powers. However, it is beyond the scope of this dissertation to consider these measures in detail and recommend the best approach or combination of approaches to effective enforcement.

[5] POPIA s 37.

2. Provide education, inter alia 'to promote an understanding and acceptance of the conditions of lawful processing of personal information and the objects of those conditions';[6]
3. Monitor compliance,[7] and report to the Minister of Justice and Parliament;[8]
4. Assess compliance by any responsible party mero motu or on request;[9]
5. Investigate and give authorisation for any processing of unique identifiers save as specifically intended upon collection for purposes of information linking,[10] and monitor, report on and make recommendations to Parliament about the use of unique identifiers;[11]
6. Maintain a register of approved codes of conduct;[12]
7. Consult with the public and national and international data supervisory authorities;[13]
8. Issue codes of conduct and enforce breach of the code as a deemed breach of the conditions for lawful processing under POPIA;[14] and
9. Facilitate cross-border cooperation.[15]

In addition to the above 'soft' regulatory measures, the Information Regulator can receive and investigate complaints,[16] refer its recommendations to the Enforcement Committee, and with its approval issue enforcement notices for breach of the Act.[17] Failure to comply with an enforcement notice is a statutory offence subject to administrative fines of up

---

[6] Ibid s 40(1)(a).
[7] Ibid s 40(1)(b)(i)-(iii). These measures include research on how the adverse effects of new technologies can be minimised, and how proposed legislation, regulations and government policy may impact data protection. Subsec (ix) specifically enjoins the Regulator to address legislation that providers for government information matching programmes, and s 40(1)(e) refers more widely to any international instruments or necessary legislative amendments that the Information Regulator considers should be adopted.
[8] Ibid s 40(1)(b)(iv)-(v). Apart from its annual report to Parliament, the Information Regulator may upon request or on its own accord report on any policy matter, including the need for legal reform.
[9] Ibid s 40(1)(b)(vi) read with s 89.
[10] Ibid s 57(1). These powers can be extended to other types of information that pose a similar risk to the legitimate interests of data subjects.
[11] Ibid s 40(1)(b)(vii).
[12] Ibid s 40(1)(b)(viii) read with s 66(1).
[13] Ibid s 40(1)(c).
[14] Ibid s 40(1)(f) read with chapter 3, chapter 7 (in particular s 68), and chapter 10.
[15] Ibid s 40(1)(g) read with chapter 9.
[16] Ibid s 40(1)(d) read with ss 74–88. This includes complaints about the breach of a code of conduct under s 63(1).
[17] Ibid s 92 and s 95.

to R10 million or imprisonment for up to 10 years.[18] In addition, breach of POPIA (whether intentional, negligent or innocent) is subject to civil action, which can be instituted by the Information Regulator at the request of the data subject.[19]

In chapter 6 the express provisions for unique identifiers as personal information,[20] and the requirements for prior authorisation when linking such identifiers to other information, were discussed.[21] POPIA creates a specific offence in relation to the use by a responsible party and any third party of an 'account number'.[22] An account number is defined to include a unique identifier, but only when it functions as an account number for access to funds or credit.[23] The offences therefore do not address the accountability of responsible parties and third parties for the processing of unique *device* identifiers such as is common in the mobile apps ecosystem.

However, the main conclusion drawn from chapters 8 and 9 is that the development of regulatory guidance to unpack the concept of PbD is a first step towards the implementation of such an approach through the development of industry standards and approved codes of conduct, adopted after consultation with all stakeholders, and which can form the basis for the effective enforcement of the overarching conditions of lawful processing.

---

[18] Ibid s 103 read with s 107(a) & s 109.

[19] Ibid s 99. Section 99(1) provides that damages can be claimed 'whether or not there is intent or negligence on the part of the responsible party'. This means that even if neither intention nor negligence is established (i.e. the responsible party innocently breached the provision in ignorance) it may be liable for damages caused by the breach.

[20] Ibid s 1 subpara (c) of the definition of 'personal information'.

[21] Ibid s 71.

[22] Section 105 provides that the responsible party is guilty of an office if it fails to ensure that processing is carried out in accordance with all conditions of lawful processing, and s 106 provides that a third party is guilty of an offence if it 'knowingly or recklessly', without the consent of the responsible party, obtains, disclosures or procures the disclosure of a data subject's account number.

[23] POPIA s 105(5) provides: ' "Account number", for the purposes of this section and section 106, means any unique identifier that has been assigned—
(a) to one data subject only; or
(b) jointly to more than one data subject,
by a financial or other institution which enables the data subject, referred to in paragraph (a), to access his, her or its own funds or to access credit facilities or which enables a data subject, referred to in paragraph (b), to access joint funds or to access joint credit facilities.'

IV PRIVACY BY DESIGN APPROACH IMPLIED UNDER POPIA

Chapter 3 set out the 'mapping' exercise undertaken by Cavoukian to illustrate how the seven foundational principles of PbD align with the FIPs,[24] and expanded that analysis in Table 4 with reference to the core data-protection principles in the OECD Privacy Guidelines.[25] The same framework is adopted in this analysis, with reference to the conditions of lawful processing contained in POPIA, and comparative reference to GDPR. Differences in terminology, and areas of uncertainty in unpacking the practical application of broad legal principles in the mobile apps context, are illustrated.

V A PROACTIVE AND PREVENTATIVE APPROACH

It is not sufficient to wait until a privacy or security breach occurs and then take action. PbD requires app developers to be 'proactive, systematic and innovative' in their approach, and to take steps to prevent the occurrence of any reasonably anticipated risk to privacy and security. App developers should be able to implement the highest possible standards of privacy and security in the design of mobile apps and throughout their organisation. App developers should work only with other role-players in the ecosystem who share these values.[26] In this way, app developers comply with the legal conditions of accountability and security.

(a) Accountability

An app developer is a responsible party under POPIA (a data controller under GDPR) as it either alone, or jointly with others, determines the purpose and means of processing personal information. In terms of the accountability principle contained in both POPIA[27] and GDPR,[28] the responsible party (data controller) is accountable for ensuring data privacy in that it must ensure that the conditions for lawful processing are all complied with at every stage of processing. Section 8 of POPIA expressly records that this duty applies both 'at the time of the determination of the purpose and means of the processing and during the processing itself'.

---

[24] A Cavoukian, *Privacy by Design The 7 Foundational Principles Implementation and Mapping of Fair Information Practices* (Information and Privacy Commissioner, Ontario, Canada, 2010).
[25] OECD, *Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data* (C(80)58/FINAL, as amended on 11 July 2013 by C(2013)79, 2013).
[26] Cavoukian at 3. The author has not explicitly 'mapped' this PbD principle to the FIPs, on the basis that a proactive approach may go beyond legal standards.
[27] POPIA s 8.
[28] GDPR art 5(2).

In other words, accountability begins when the app is first conceptualised, as this is when the purpose and possibly the means of processing personal information will be determined. Thus, privacy and security considerations must be considered from the very beginning of the design process. Further accountability is continuous, in that it applies 'during the processing'.[29] Accountability begins as soon as personal information is collected and ceases only at the end of the data lifecycle, when the data is deleted or otherwise completely de-identified.[30] This implies a PbD approach.

PbD requires that there should be no gaps in protection. The app user, downstream processors, and upstream technology service, product and platform providers are all distinct role-players in the ecosystem. However, where they will receive personal information from the app, and process this for their own purposes, they then become a responsible party in their own right.

Where those purposes are additional to or separate from the purposes of the app developer, then, from the perspective of the app developer, any transfer of personal information should be treated as a transfer to a third party, which triggers notice and consent obligations in order to comply with the conditions for lawful processing. In chapter 10, recommendations are made for the introduction of additional legislative provisions in POPIA to strengthen this obligation.

(b) Security

The legal obligation to ensure the security of personal information is expressed in POPIA and GDPR as an obligation to ensure the integrity and confidentiality of personal information.[31] In other words, personal information must be protected against loss, degradation, unauthorised destruction, transmission or other processing of personal information.[32]

The security obligation is integral to the protection of personal information, and by definition implies a proactive and preventative approach in that security measures must be adopted from the outset to prevent any reasonably foreseeable risk of data loss or data breach. In accordance with the principle of accountability, the security obligation is continuous, in that

[29] POPIA s 8.
[30] POPIA s 1, definition of 'de-identify'.
[31] POPIA s 19(1) and GDPR rec 78 and art 5(1)(f).
[32] POPIA s 19(1) and GDPR art 32(2).

it applies throughout the data lifecycle, and comprehensive, in that it applies to any risk that would compromise full compliance with the conditions of lawful processing.

This includes both internal and external risks,[33] and risks at any stage of data processing, including the collection, transmission, use, storage or deletion of personal information. POPIA and GDPR are technologically neutral legislation and refer only to '*appropriate* technical and organizational measures'.[34] Section 19(1) of POPIA simply states that such measures must be reasonable. Article 25(2) of GDPR sets out four factors that must be taken into account in determining and implementing such measures:

> *'the state of the art, the cost of implementation, the nature, scope, context and purposes of processing and the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing'.*

Each of these factors must be considered in relation to any particular mobile application.

VI PRIVACY AS THE DEFAULT

A PbD approach requires that the default settings of any mobile app are 'the most privacy protective'.[35] By default, the mobile app should not collect any personal information, unless the app user has been notified of what is being collected, and how it will be used, and there is a lawful basis for the processing.

This principle may well be the most important contribution of PbD to the effective protection of personal information. Users are often ignorant of, or apathetic about, implementing privacy controls and can easily be overwhelmed when the onus is placed on them to check privacy policies, and adjust privacy settings that make personal information shareable or public by default. Conversely, carefully designed default settings that require the user to agree actively to the collection and use of data provide an invaluable touchpoint to sensitise users to the control of their personal information, and make it easier for them to use technology in privacy-protective ways.

---

[33] POPIA s 19(1).
[34] Ibid.
[35] Cavoukian at 3. Again, although the terms used may suggest otherwise, it is clear from the overall tenor of PbD that user privacy is not to be at the expense of full functionality. PbD calls for innovative design that can provide that functionality while protecting privacy to the fullest extent reasonably possible.

As technologically neutral legislation, POPIA and GDPR do not specify how default settings must be configured, but the data-minimisation principle restricts how much personal data may be collected,[36] used[37] and stored by,[38] and made accessible to, third parties.[39]

(a) Data Minimisation

Both POPIA and GDPR require that all processing, including the collection of personal information, be 'adequate, relevant and not excessive';[40] in other words, it must be data that are necessary for the specified purposes of processing.

(b) Purpose Specification

POPIA and GDPR expressly provide that the collection of personal information is limited to what is required for a 'specific, explicitly defined and lawful purpose'.[41] POPIA goes even further than GDPR in explicitly limiting the purposes to ones that are 'related to a function or activity of the responsible party'.[42]

(c) Lawfulness and Reasonableness

The OECD Guidelines require that personal information 'should be obtained by lawful and fair means'.[43] The requirement of lawfulness and fairness is extended to all processing in GDPR.[44]

---

[36] POPIA s 13(1) ('Purpose specification'), GDPR art 5(1)(b) ('Purpose limitation'), OECD Guidelines principle 1 ('Collection limitation'), principle 3 ('Purpose specification') and principle 4 ('Use limitation').
[37] Ibid.
[38] POPIA s 14(1). GDPR art 5(1)(f).
[39] OECD Guidelines principle 4. Transfers to operators (processors) is regulated in detail under POPIA ss 20 and 21 and GDPR arts 28 and 29. Transfers to third parties can only be undertaken with notice about the recipients or categories of recipients of the data in terms of POPIA s 18(1)(f)(i) and GDPR art 13. The third party who processes personal information for their own purposes are a responsible party, and having received the personal information from a source other than the data subject, they must ensure compliance with POPIA s 12 and GDPR art 14, and that their processing is lawful on the basis of the data subject's consent, or under the grounds of legitimate interests of the responsible party.
[40] POPIA s 10. GDPR art 5(1)(c) states in similar terms that data must be 'adequate, relevant and limited to what is necssary.
[41] POPIA s 13(1). GDPR art 5(1)(b) expresses the same obligation referring to 'specified, explicit and legitimate' purposes. It is purely semantics that this principle is referred to as 'purpose specification' in POPIA, 'purpose limitation' in GDPR. The principles cover much the same ground as the principles of 'Collection limitation', 'Purpose specification' and 'Use limitation' in the OECD Guidelines, but go somewhat further in defining more clearly that purpose limits both collection and use of personal information, and incorporating the principle of minimality, building on art 5(b) and (c) of the COE Convention 108 which express the same principles under the heading 'Data quality'.
[42] POPIA s 13(1).
[43] OECD Guidelines principle 1.
[44] GDPR art 5(1)(a).

Similarly, POPIA requires that processing must be undertaken 'lawfully'[45] and 'in a reasonable manner that does not infringe the privacy of the data subject'.[46] This closes the door on indiscriminate data collection for undefined or loosely conceived future purposes.

(d) Notice and Consent

The OECD Guidelines provided that 'where appropriate, personal information should only be collected with the knowledge or consent of the data subject'.[47] In both GDPR and POPIA, this requires, firstly, that the user should be informed of and freely consent to the specified purpose unless it is otherwise permitted by statute;[48] and secondly, that further processing of data must be compatible with the purpose for which it was collected.[49] Aligned with this processing limitation is a storage limitation in that data must not be kept in a form which permits identification of the data subject for longer than is necessary for achieving the purpose.[50] Data should therefore be deleted, or, if this is not possible, de-identified (anonymised), or at least pseudonymised as soon as possible.[51] Thus, by default, privacy is protected.

(e) Further Processing Limitation

Both POPIA and GDPR restrict any further processing of personal information to purposes that are compatible with the original purpose for which the information was collected.[52] Vague (blanket) consent does not meet the requirement of purpose specification,[53] and further processing which is not compatible with the original consent terms requires fresh consent, unless otherwise permitted by statute.

The ability to develop secondary uses from analysis of very large data sets ('big data') presents challenges as to how core data protection principles are applied in practice.[54]

---

[45] POPIA s 9(1)(a). Processing will only be lawful if it complies with all 8 conditions of lawful processing, and does not infringe the right to privacy or the data subject's rights under POPIA.
[46] POPIA s 9(1)(b).
[47] OECD Guidelines principle 1.
[48] POPIA s 11 and GDPR art 6.
[49] POPIA s 14 and GDPR art 5(1)(b).
[50] POPIA s 14 and GDPR art 5(1)(e).
[51] European Union Agency For Network and Information Security at 50.
[52] POPIA s 15(1) and GDPR art 5(1)(b).
[53] Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers* (March 2012) at 58.
[54] Article 29 Data Protection Working Party, *Statement on the impact of the development of big data on the protection of individuals with regard to the processing of their personal data in the EU* (WP 221, 16 September 2014) at 2.

Innovation inherently involves extracting insights from data that may lead to new uses that were not anticipated at the time of collection. Following extensive debate in health ethics literature about the adequacy of broad (wide) consent versus blanket consent for future research use of biomedical specimens,[55] proposals have emerged for dynamic consent. Dynamic consent means 'personalised, online consent and communication platforms' that facilitate ongoing communication and user control.[56] Such models may be informative for privacy design in the mobile ecosystem.

(f) De-identification

Although de-identified (anonymised) data is no longer *personal* data and is thus not subject to data protection laws,[57] there is a blurred boundary between personal information and anonymous data.[58] Anonymisation is described as 'a process through which identifying information is manipulated (concealed or deleted) to make it difficult to identify data subjects'.[59] Data can be anonymised, for example, by aggregation of data or by adding 'noise'.[60] However, if there is even a possibility that data can be re-identified to link it to an individual, the data protection law applies[61]. Data are not de-identified or anonymous if the means of re-identifying an individual by manipulating the data or linking it to other data is 'reasonably foreseeable'[62] or 'reasonably likely'.[63]

The Directive on Privacy and Electronic Communications[64] requires that 'traffic data be erased or made anonymous when it is no longer needed for the purpose of the transmission of a communication'.[65] The proposed e-Privacy Regulation[66] requires that

---

[55] Isabelle Budin-Ljøsne and others, 'Dynamic Consent: A Potential Solution to some of the Challenges of Modern Biomedical Research' (2017) 18 *BMC Medical Ethics* 1–10 at 2.
[56] Ibid at 3.
[57] POPIA s 6(1)(b) and GDPR rec 26.
[58] Federal Trade Commission at 2.
[59] Samson Esayas, 'The Role of Anonymisation and Pseudonymisation under the EU Data Privacy Rules: Beyond the 'All or Nothing' Approach' (2015) 6 *European Journal of Law and Technology* 1–28 at 4. See discussion in chapter 2.
[60] European Union Agency For Network and Information Security at 48.
[61] Esayas at 10.
[62] POPIA s 1.
[63] GDPR rec 26.
[64] Directive 2002/58/EC of the European Parliament and of the Council on privacy and electronic communications OJ L 173, 26.6.2013 (e-Privacy Directive).
[65] Ibid art 6(1).
[66] Proposal for a regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) Brussels, 10.1.2017 COM (2017) 10 final 2017/0003 (COD).

electronic communications data (which includes both content and metadata) be made anonymous unless the data subject has consented to the processing and the purpose of processing cannot be fulfilled by processing anonymous data.[67] POPIA requires that 'data must not be kept in a form which permits identification of the data subject for longer than is necessary for achieving the purpose' for which it was collected and processed.[68] This can be achieved by destroying, deleting or de-identifying a data record.[69]

Pseudonymisation, on the other hand, can be achieved 'by replacing names or other direct identifiers with codes or numbers' to prevent an individual from being identified.[70] Data have been pseudonymised if technical and organisational measures are implemented to ensure that additional information that could be used to attribute the data to a specific data subject is always kept separately.[71] Pseudonymisation of data is specifically encouraged under GDPR[72] as a practice which can protect privacy, although this does not preclude other measures such as encryption. While pseudonymisation is not explicitly referred to in POPIA, it is a PbD practice that may be used to achieve privacy objectives of a responsible party. However, parties subject to POPIA are considerably constrained in their ability to make use of pseudonymised data by the requirement in section 14(4) that the data be deleted or de-identified (which by definition requires deletion of any information that could reasonably be used to re-identify an individual) once the responsible party is no longer authorised to retain the data. Consent to retain the data in a pseudonymised form for a longer period would be required.

VII PRIVACY EMBEDDED INTO DESIGN

App developers should design mobile apps to protect the privacy of mobile app users. This involves the systematic adoption of 'accepted standards and frameworks',[73] subject to independent review or audit, and internal privacy impact assessments. The aim of the design

---

[67] E-Privacy Regulation art 6(2)(c) and 6(3)(b).
[68] POPIA s 14(1).
[69] POPIA s 14(4).
[70] Esayas at 4.
[71] GDPR art 4.
[72] Ibid art 25(1).
[73] Cavoukian at 3, recognises that PbD requires consideration of the 'broader context' and consultation of 'all stakeholders and interests', i.e. it is an eco-system wide approach. However, she also calls for creative invention of new alternatives where existing solutions are unacceptable from the privacy perspective.

process should be to demonstrate minimal privacy impacts considering anticipated use, and possibilities for misconfiguration or error.[74]

The limits on the collection, use, disclosure and retention of personal information (data minimisation) discussed above apply with equal force to this PbD objective. Thus every item of personal information that will be collected by the mobile app must be tracked to a specific, explicit, lawful purpose, or the app must be redesigned to avoid the collection of that personal information.

VIII FULL FUNCTIONALITY – POSITIVE SUM, NOT ZERO SUM

PbD calls for app developers to design innovative solutions to embed privacy while permitting full functionality.[75] App developers should clearly document the interests and objectives of the app user and app owner/developer and the desired functions of the app, in order to achieve this objective.[76]

(a) Proportionality

POPIA and GDPR recognise the need to balance the data subject's right to privacy against the legitimate interests of the responsible party and third parties. However, this balancing exercise must be undertaken in a constitutionally sound manner, recognising that the right to privacy is a fundamental human right, and that the economic interests of the app developer/app owner and third parties can be pursued only if there are adequate safeguards to protect the privacy of the app user. Placing users in a position where they must agree to forgo the privacy of their personal information in order to use the app does not strike an appropriate balance, when it is possible for the app to function without the collection of the information.

IX END-TO-END LIFECYCLE PROTECTION

PbD requires that there should be 'no gaps in protection or accountability'.[77] App users must apply recognised security standards, including secure destruction, encryption, access controls

[74] Ibid.
[75] Ibid.
[76] Ibid.
[77] Cavoukian at 4.

and logs, to ensure 'confidentiality, integrity and availability' of personal data 'across the entire domain and throughout the life-cycle of the data'.[78]

(a) Data Quality

The principles of accountability and security, discussed above, are directly applicable and provide for this end-to-end protection of personal information. The principle of data integrity is informed further by the requirement that a responsible party must take 'reasonable steps' to ensure that the personal information is 'complete, accurate, not misleading, and updated where necessary'.[79]

X VISIBILITY AND TRANSPARENCY

A PbD approach requires app developers to operate 'according to stated promises and objectives'.[80] When using third-party software or services, measures should be employed to verify independently that those parties also adhere to stated privacy and security standards.[81]

(a) Openness

The principle of openness requires the app developer to document its compliance with the Act,[82] and provide transparent notice to data subjects.[83] Privacy policies and terms of use as well as internal policies and procedures should be drafted to comply with these requirements.

(b) Data Subject Participation

POPIA and GDPR require an app developer to comply with all conditions of lawful processing, and to give effect to the data subject's rights.

---

[78] Cavoukian at 4.
[79] POPIA s 16(1) ('data quality'). GDPR art 5(1)(d) ('accuracy') requires personal data to be 'accurate, and, where necessary, kept up to date' and inaccurate data is to be erased or rectified 'without delay.'
[80] Cavoukian at 5. Privacy policies and procedures must be documented, kept up to date and available, and assigned to the responsibility of a person within the organisation. Contractual safeguards must be implemented when disclosing personal information to third parties.
[81] Ibid.
[82] POPIA s 17. GDPR art 30.
[83] POPIA s 18. GDPR arts 12–14.

XI RESPECT FOR USER PRIVACY

A PbD approach requires app developers to design technology interfaces and develop organisational processes and procedures that are 'user-centric' and 'user-friendly'.[84]

Guidelines on best practice for mobile app developers provide examples of how to obtain informed consent.[85] Informed consent requires a 'clear affirmative act'[86] and must be preceded by disclosure of a specific, explicit and legitimate purpose.[87] Blanket acceptance of general privacy terms does not meet the requirements for valid consent under GDPR[88] or POPIA.[89] While the challenges of communicating privacy practices on a small mobile screen are widely acknowledged, consent notifications must still be clear, prominent and delivered at an appropriate time.[90]

Valid consent involves a subjective enquiry into whether a user willingly consents when he or she knows and understands what personal information the app will collect, how it will be used, and the risks or consequences to the user of doing so. For the app developer designing the settings used to obtain or withdraw consent, or exercise any other data subject rights, this legal objective can be met by adopting a user-centric mindset to design user-friendly interfaces.

XII PRACTICAL APPROACHES TO PRIVACY BY DESIGN

Table 5 summarises the discussion above and provides some insight into the challenges of providing practical guidelines to app developers on the design requirements indicated for compliance with broad legal principles. The table presents an analysis undertaken by ENISA[91]

---

[84] Cavoukian at 4.
[85] National Telecommunications and Information Administration (NTIA) US Department of Commerce, *Short Form Notice Code of Conduct to Promote Transparency In Mobile App Practices* (2013 July 25) and Future of Privacy Forum and Center for Democracy and Technology, *Best Practices for Mobile Applications Developers* (December 2011). See further detailed discussion of the implementation of PbD through self-regulation in chapter 7.
[86] GDPR art 4(11). It is argued in chapter 6 that this is also implied by the elements of valid consent under POPIA.
[87] POPIA s 13(1) and GDPR art 5(1)(b).
[88] Article 29 Data Protection Working Party, *Guidelines on Consent under Regulation 2016/679* (WP 259, 28 November 2017) at 16. See further the discussion of consent in GDPR in chapter 5.
[89] See discussion of consent in POPIA in chapter 6.
[90] Federal Trade Commission at 58. Also see GSM Association (GSMA), *Mobile Privacy Principles: Promoting Consumer Privacy in the Mobile Ecosystem* (January 2011) at 5.
[91] European Union Agency for Information Security (ENSIA), *Privacy and Data Protection in Mobile Applications: A Study on the App Development Ecosystem and the Technical Implementation of GDPR* (November 2017) at 22.

of the application of GDPR principles in the context of mobile applications. Column 1 of Table 5 has been inserted to show the close correlation between the GDPR and POPIA. Row 8 of Table 5 has been added to show the accountability principle contained in the legislation.

TABLE 5 AN INDICATIVE EXAMPLE OF ASSESSING RISKS WITH REGARD TO LEGAL COMPLIANCE

POPIA CONDITION	**GDPR PRINCIPLES**	**INDICATIVE PRIVACY RISKS**	**INDICATIVE REQUIREMENTS**
Processing Limitation Lawful and reasonable (Sec 9) **Openness** (Secs 17 & 18) **Data subject participation** (Secs 23–25)	Lawfulness, fairness and transparency (Art 5(1)(a))	Unlawful, excessive and incorrect processing (e.g., due to permissions to unauthorised parties to access personal data through the app).	App providers/developers should make sure that they have a legal basis for the processing of personal data. App providers/developers should inform the data subjects properly about their data processing activities. This may help the users to understand what personal data is collected by them and why. App providers/developers should be aware of data subject rights such as rights to access, rectification, erasure, data portability. They should implement appropriate processes to support these rights. Transparency requires the documentation of processing operations
Purpose specification Sec.13 **Further processing limitation**	Purpose limitation Art.5(1)(b)	Excessive collection and sharing of data (e.g., due to multiple sensors of mobile devices that are activated without need).	App providers/developers should use the data for a specific purpose of which the data subjects have been made aware, and no other, without further consent. If the personal data are used for purposes other than the initial purpose, they should be anonymised or

Sec.15			the data subjects must be notified and their consent must be re-obtained.
Processing Limitation Minimality Sec.10	Data minimisation Art.5(1)(c)	Excessive processing (e.g. due to use of third-party libraries).	The minimum amount of data for specific processing should be processed by app providers/developers. For instance, they should not store the exact location point when a generic location area is sufficient for their app functionalities.
Information quality Sec.16	Accuracy Art.5(1)(d)	Outdated data pose identity theft risks.	Rectification processes into data management should be embedded in the app design.
Processing Limitation Retention & restriction of records Sec.14	Storage limitation Art.5(1)(e)	Undue data disclosure (e.g. due to cloud storage services used by mobile app developers).	Personal data must not be stored longer than necessary. App providers/developers should provide the 'right to be forgotten' to the data subjects. This data must be kept only for a certain period of time for non-active users.
Security safeguards Sec.19 & 20	Integrity and confidentiality Art.5(1)(f)	Unlawful data processing, data loss, data breach, data destruction or damage	App providers/developers should ensure that the security requirements of the personal data and the processing systems are met. This encompasses integrity and confidentiality as well as availability and resilience (Art. 35(1)(b) GDPR). For instance, the appropriate control access mechanisms should be embedded into the apps infrastructure in order to detect or monitor unauthorised access to the data.

Accountability Sec. 8	Accountability Art 5(2)	The responsible party/controller must ensure that the conditions for lawful processing are complied with.	Use trusted third parties but verify that privacy policies will be respected.

Source: Col 1 & row 8 adapted from POPIA 2013; Botha et al. 2015:41; Col 2–4, rows 1–7 drawn from ENISA 2018:22.

XIII CONCLUSION

This chapter has concluded that although there is no explicit obligation to implement PbD under POPIA, such an approach is implied and would be required for compliance with the conditions of lawful processing under POPIA. However, the accountability gap identified in earlier chapters in relation to the US and the EU, is also inherently problematic for the implementation of PbD under POPIA in South Africa. A fortiori where one considers that Pb(re)D of existing technologies and systems requires clear legal duties to be imposed on all roleplayers, it is essential that accountability be adequately addressed in the legislation. In the final chapter, drawing on the comparative analysis with the US and EU data protection laws considered in this dissertation, amendments to strengthen the legal obligations of the responsible party are recommended. These amendments do not include the introduction of a similar provision to article 25 of GDPR. Rather, they involve strengthening legal obligations as a necessary preliminary step to later developing concretised PbD objectives in industry codes of conduct and technical standards.

CHAPTER 10

CONCLUSION

I INTRODUCTION

This dissertation presented a comparative legal analysis of selected data protection instruments in the US, the EU and South Africa. It adopted the conceptual framework of privacy by design (PbD), which requires that privacy be embedded directly in technology through default settings that permit full functionality while protecting user privacy.

In relation to its central hypothesis, this study has theorised that the adoption of a PbD approach by a responsible party is impliedly necessary in order to comply with the conditions of lawful processing set out in POPIA. This chapter sets out the comparative conclusions to be drawn from the analysis of the principles of PbD and the data protection principles in the US,[1] EU[2] and South African law.

As app developers must develop within a complex ecosystem in adherence with standards imposed by existing technologies and platforms, privacy by (re)design can be achieved effectively only through an ecosystem-wide approach. However, in all three jurisdictions considered, it was concluded that there is an 'accountability gap'. Accountability is directly imposed on the party which is responsible for ensuring compliance by downstream processors through contractual means. However, upstream technology and platform providers are not accountable under existing data protection statutes, save to the extent that they process personal information themselves.

---

[1] Children's Online Privacy Protection Act of 1998, 15 U.S.C. §§ 6501 - 6506 (2018) (COPPA) and the Children's Online Privacy Protection Rule, 16 C.F.R part 312 (COPPA Rule) (COPPA), The Online Privacy Protection Act of 2003, Cal. Bus. & Prof. Code §§ 22575–22579 (2004) (CalOPPA) and The California Consumer Privacy Act of 2018, Cal. Civ. Code §§ 1798.100 - 1798.199 (CCPA) (CCPA).

[2] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA OJ L 119, 4.5.2016 (EU General Data Protection Regulation; GDPR).

II SUMMARY OF CHAPTERS

Chapter two set out key terminology, and a description of the role-players and data processing practices used within the mobile applications ecosystem. It illustrated the complexity in data processing practices, and to highlight the need to engage all stakeholders and illustrate that the privacy of app users cannot be ensured by app developers alone.

Chapter three discussed the relationship between the core principles underpinning data protection laws and the seven foundational principles of PbD. While PbD has widespread approval from data protection authorities, a PbD approach needs concrete articulation in both enforceable legal obligations and defined software development goals. The data protection principles of data minimisation and accountability were identified as being at the heart of an effective PbD approach, and thus equally important to the achievement of Pb(re)D of the existing technologies and systems upon which mobile apps are built.

Chapters four, five and six considered selected data protection laws in the US, EU and South Africa respectively. The chapters defined the concepts of personal information, the responsible party, consent, other grounds for lawful processing, and notice in the relevant legislation, and discussed the principles of accountability and data minimisation.

Chapter seven provided a critical analysis of the PbD guidelines issued to mobile application developers in the US. The chapter illustrated that industry self-regulation and advocacy measures alone are insufficient to compel compliance with a Pb(re)D approach by all role-players within the mobile app ecosystem. Despite robust regulatory action and class action law suits in the US, there remains a gap in relation to processing by third parties and the accountability of upstream technology and platform providers. The US approach indicates that widespread stakeholder engagement is required to develop regulatory guidance that move beyond textual restatements of existing legal principles to agreement on industry standards.

Chapter eight provided a critical analysis of the implementation of PbD through the adoption of article 25 of GDPR, which imposes an express duty on data controllers to ensure data protection by design and by default. The shortcomings of this approach for the implementation of clear legal duties on all legal roleplayers to adopt a Pb(re)D approach were discussed.

Chapter nine presented the conclusion that a PbD approach is required for compliance with POPIA, but that the accountability gap inherent in POPIA is an impediment to the succesful implementation of Pb(re)D in the mobile apps ecosystem.

III COMPARATIVE CONCLUSIONS

Each of the jurisdictions studied bases its data protection laws to some degree on a set of broadly similar data protection principles (also known as fair information practices or conditions of lawful processing). However, the substance of those principles varies on closer analysis in ways that could make it complex for mobile app developers to comply with laws across multiple jurisdictions (particularly where laws apply extra-territorially). This study has examined the key concepts of personal information, the responsible party, consent, other grounds of lawful processing and notice to be given to the data subject. The study has considered in depth the two data protection principles that lie at the heart of a PbD approach: data minimisation and accountability.

(a) Personal Information

The US legislation considered applies to the personal information respectively of a child[3] and a natural person who is a consumer resident in California,[4] or their household,[5] regardless of where the operator/business is situated or where the processing takes place. GDPR and POPIA apply to the personal information of any living, natural person, and, in the case of POPIA, also, where applicable, to an existing, identifiable juristic person.[6]

Location information and device identifiers are particularly relevant in the context of online services such as mobile apps. As explained in chapter 2, this is the most common means of linking personal information in a profile about an individual. There are differences in the granularity of location data regarded as personal information[7] and the terminology used regarding device identifiers.[8] It is submitted that as none of the statutes purports to create a closed list, there is a measure of flexibility that permits a wide

[3] COPPA Rule 16 C.F.R §312.2.
[4] CalOPPA §22577(d) and CCPA §1798.140(o)(1).
[5] CCPA.
[6] GDPR art 4(1) and POPIA s 1.
[7] COPPA Rule 16 C.F.R §312 and CalOPPArefers to 'precise' geolocation data, CCPA §1798.140 (o)(1)(G) refers to 'geolocation data' and GDPR art 4(1) and POPIA s 1 refer to 'location' information. CalOPPA does not refer to location information at all.
[8] COPPA Rule 16 C.F.R §312.2 refers to a persistent identifier that is used to identify an individual across time or across services. CalOPPA §22577(a) refers to a persistent identifier that permits physical or online contacting of a specific individual. CCPA §1798.140(g) refers to any unique identifier that can identify a consumer or their household and §1798.140 (o)(1)(A) also refers to a 'unique personal identifier' and an 'online identifier'. GDPR art 4(1) and POPIA s 1 refer to an 'online identifier'.

interpretation.[9] GDPR and POPIA apply to any location information or online identifier (if an individual is directly identified or indirectly identifiable from the information).[10] It is submitted that both terms should be interpreted widely to include any data or metadata from which a data subject's location or identity can be extrapolated.

(b) Responsible Party

Each of the instruments studied imposes obligations on the responsible party (data controller/operator/business). Despite some differences in how this party is identified, in the mobile apps ecosystem, it would include the app developer, or the app owner, where the development is outsourced.[11] In the latter instance, it appears unclear whether the app developer shares statutory liability for a breach of the data protection laws that occurs as a result of the app design. In any event, they may face an action for damages or an indemnity if their client is exposed to liability arising from the app developer's failure to address data protection in the design of the app and should accordingly adopt a PbD approach, but may also seek appropriate contractual indemnities and exclusions of liability from their client.[12]

(c) Data Protection Principles

The seven foundational principles of PbD, which form the theoretical framework for this dissertation, were discussed in chapter 3, and are closely aligned to the data protection

[9] In each case the general principle is that an individual is identified or identifiable from the information, and include (but are not restricted to) the examples listed.

[10] GDPR art 4(1) and POPIA s 1. Also see Article 29 Data Protection Working Party, *Opinion 4/2007 on the concept of personal data* (WP 136). Cf Children's Online Privacy Protection Rule; Final Rule Amendments, FR 79(12) Part II (17 January 2013) at 3979 (fn 79) where public comments assert that under COPPA information must relate directly to an individual, and the CCPA which refers to either an individual or a household.

[11] In the latter instances if the app developer is retained after the app is deployed to operate the service on behalf of the app owner, it is submitted that legally they should be classified as what POPIA terms an 'operator' (a 'processor under GDPR and a service provider under US law).

[12] CalOPPA §22577(c) restricts statutory liability to the owner of a website or online service. COPPA Rule 16 C.F.R §312 and CCPA includes as an 'operator' the party that collects or maintains the personal information collected on a website or online service, even if this is done on their behalf. Ibid §1798.140(c)(1). Hence the developer who acts on behalf of POPIA the app owner should be viewed as a service provider, and the app owner as the 'operator' (responsible party). s 1 and GDPR art 4(7) define the responsible party (data controller) as the party that determines the purpose and means of processing, alone or jointly with others. Although a developer may determine the purpose or means of processing (from a technical perspective) where they do so as the independent subcontractor of the app owner, the app owner should be viewed as the responsible party. However this view is open for argument.

principles. That relationship, drawing on the framework developed by Cavoukian,[13] was presented in chapter 3.

The discussion in chapters 4, 5 and 6 demonstrated that the fair information practice principles (FIPPs) applied in the US are more restricted than the broader list of data protection principles contained in GDPR and POPIA, which are underpinned by accountability to justify the lawfulness of processing and the processing limitations imposed by the principle of minimality.

Chapter 7 demonstrated that PbD is enforceable only to the extent that it creates a legal obligation. However, chapter 8 concluded that introducing a 'vague' general obligation to implement data protection by design and by default is potentially unworkable without the development of appropriate industry standards.

In the context of South Africa, Europe and California, the principles of PbD as articulated by Cavoukian are entrenched in a constitutional right to the protection of privacy. Europe also confers a right to data protection. In South Africa's constitutional dispensation, this requires balancing the right to privacy against other rights (such as freedom of expression and access to information) and other important interests (including the legitimate interests of the mobile app developer in the efficient operation of their business). Privacy as a fundamental right closely aligned to dignity holds great weight and it is submitted that an infringement of privacy would ordinarily trump the app developer's legitimate interests on an application of a limitation enquiry pursuant to section 36 of the Constitution.

Consent is accordingly key in borderline cases. Only the voluntary, specific and informed consent of the data subject can legitimise processing that would otherwise constitute an infringement of the right to privacy. Notice is central to the existence of informed consent and to the exercise of data subject rights. The overarching principles of data minimisation and accountability are central to the PbD requirements of privacy by 'default' and privacy throughout an ecosystem. In considering the extent to which a PbD approach is required for compliance with POPIA, the following five issues were considered in detail.

---

[13] A Cavoukian, 'Privacy by Design The 7 Foundational Principles Implementation and Mapping of Fair Information Practices' <https://iab.org/wp-content/IAB-uploads/2011/03/fred_carter.pdf> accessed 17 September 2019.

(d) Consent

There are wide differences in how data protection statutes approach consent. On the one hand GDPR and COPPA expressly require granular opt-in consent either by a consent statement or some other action that indicates that they do give their consent to each specific purpose of processing.[14] Under POPIA, this is implied by the requirement that consent should be an 'expression of will',[15] that there should be voluntary, specific and informed consent[16] given for a specific and explicitly defined purpose,[17] and that the data subject must be made aware whether the collection is voluntary or mandatory.[18]

Although there are differences in wording between COPPA, GDPR and POPIA, it is submitted that they all require consent to be:

1. given prior to processing (that is, before any personal information is collected);[19]
2. given affirmatively (that is, by 'opt-in' rather than 'opt-out' mechanisms, where the default setting requires user action before any information is collected);
3. given for clearly specified purposes which have been adequately explained; and
4. given freely (that is, any collection that is not reasonable and necessary for the use of the service is not unfairly made a condition of use of the service).[20]

At the other extreme, CalOPPA requires only notice, and consent to processing can be implied from the data subject's passive use of the service. Silence or inaction by the data subject satisfies the requirement of consent. The responsible party does not need to document or log any action by the data subject to prove that its processing is lawful on the basis of valid consent; nor is it required to provide an opt-out mechanism.

---

[14] GDPR art 4(11) read with art 7, art 13(2)(e) and rec 42. COPPA Rule 16 C.F.R §312.5.
[15] POPIA s 1 definition of 'consent'.
[16] Ibid.
[17] Ibid s 13(1).
[18] 18(1)(d) & (e).
[19] COPPA Rule 16 C.F.R §312(a)(1). In GDPR this is implied from the use of the past tense ('has given consent') in art 6(1)(a).
[20] These four criteria are expressed in similar terms in relation to Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (Data Protection Directive) OJ 1995 L 281/31, 23.11.1995in Article 29 Data Protection Working Party, *Working Document 02/2013 Providing Guidance on Obtaining Consent for Cookies* (WP 208, 2 October 2013) at 3.

In between these two poles, the CCPA provides that consent cannot be made conditional upon the consumer agreeing to the sale of personal information, and a consumer must be notified of the right to opt out.[21] All consumers must be given 'explicit notice' if third parties will on-sell personal information and must be notified of the right to opt out.[22] Thus prior opt-in consent is not required, but the CCPA imposes a requirement that every website and privacy policy should display a clear, conspicuous notice of the opt out, titled "Do Not Sell My Personal Information", with a link to the opt-out page.[23] Thus silence or inaction by the data subject implies consent, but the law stipulates detailed steps designed to inform consumers about an easy-to-use opt-out mechanism.[24]

(e) Other Grounds of Lawful Processing

Under COPPA, the only exception to the consent requirement is where information is released to a service provider who will process the information only for the purpose of providing support for internal operations of the service,[25] such as debugging, security measures, and contextual advertising. A parent must be given the option to use the service but should refuse consent for disclosure to third parties.[26]

Under POPIA and GDPR, the ground of processing on the basis of contractual necessity and the legitimate interests of the responsible party/controller are two important exceptions to the requirement of consent. Consent is not required for the processing to be lawful, but in the context of the service and notice given, it must be clear that the data subject would understand that the processing is necessary for the service. Consistent with the US approach, consent would be implied if the data subject then uses the service. The concept of 'legitimate interests' is undefined and open ended, but it is submitted that it must be interpreted in such a way that reasonable restrictions are imposed. Consistent with the US approach, processing for internal operations would be lawful, but processing for direct marketing or disclosure to third parties would require prior consent.

---

[21] CCPA §1798.105(b) read with §1798.130.
[22] Ibid §1798.115(d).
[23] Ibid §1798.135(a)(1) & (2).
[24] Ibid §1798.125(a)(3) requires prior opt-in consent only for financial incentive schemes.
[25] COPPA Rule 16 C.F.R §312 §312.2 definition of 'release', 'disclosure', 'third party' and 'internal support' functions.
[26] Ibid §312.5(a)(2).

Consent is always required to process the content of communications, and to disclose metadata (traffic data and location) to third parties under the e-Privacy Directive[27] in the EU and RICA[28] in South Africa. RICA's provisions are less extensive in that there is no requirement to anonymise traffic data when it is no longer needed,[29] to minimise the collection and purposes of processing and storage,[30] and in particular, as highlighted in chapter 6, there is no requirement for consent to read information from or write information to the user's device.[31]

(f) Notice

All the laws require notice, and the requirements as to content of that notice are broadly similar in the statutes studied.[32] Notice covers future processing, but fresh notice is required if different types of personal information are collected, or if the purpose of processing (including disclosure to third parties) changes.[33] Further, although POPIA does not contain the detailed prescriptive provisions about the modalities and contents of valid notice set out in other statutes studied, there is adequate protection in that the responsible party must:

1. have an Information Officer;[34]
2. document processing operations;[35]
3. produce a PAIA manual setting out, inter alia, prescribed information about the collection, use and disclosure of personal information;[36]
4. make its PAIA manual available on its website (if any), as well as at its principal place of business, and on request, to the Information Regulator or any other person;[37]

[27] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector 2002/58/EC (e-Privacy Directive) OJ L 201/37, 31.7.2002See art 5(1) & art 6.
[28] Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 of 2002 (RICA), s 2 & s 14.
[29] e-Privacy Directive 2002/58/EC art 6(1).
[30] Ibid art 6(2) & 6(4).
[31] Ibid art 5(3).
[32] As explained in chapter 6 the provisions of POPIA s 18, must be read together with s 51 of the Promotion of Access to Information Act 2 of 2000 (PAIA) and s 43 of the Electronic Communications and Transactions Act 25 of 2002 (ECTA).
[33] POPIA s 18(3).
[34] Ibid s 55.
[35] Ibid s 17.
[36] PAIA s 51.
[37] Ibid s 51(3).

5. take reasonably practicable steps to ensure that the data subject is aware of the contents of the notice (compliance likely requires at a minimum clear and conspicuous notice on its webpage, and the home screen and settings of the app);[38] and

6. ensure (insofar as the data subjects are consumers) that notice is worded in plain and understandable language, supported by a clear visual layout, and use of clear illustrations, examples and headings.[39]

The key difference revealed by the detailed discussion in chapter 6 was that POPIA provides wider exceptions to the requirement to give notice than the other laws considered. Recommendations for suitable amendments are discussed further below.

(g) Data Minimisation

A key issue identified in this study is that the data minimisation principle is expressed differently in different instruments. On the one hand, this is expressed as requiring that data collection be restricted to a 'strict minimum' of what is necessary for the core functions of the service. Statements to this effect appear in PbD policy documents,[40] guidance by industry organisations and privacy advocacy groups such as W3C[41] and EPIC,[42] and in the e-Privacy Directive.[43]

---

[38] POPIA s 18(1). Cf the express obligations in COPPA Rule 16 C.F.R §312 §312.4(d); CalOPPA §22577(b)(1); CCPA §1798.135(a)(1) and GDPR art 12.

[39] Consumer Protection Act 68 of 2008 (CPA) s 22. Cf the express obligations in COPPA Rule 16 C.F.R §312.4(a) and GDPR art 12. The CCPA 1798.185(a)(6) provides for such matters to be dealt with in regulation. Cf POPIA s 112 does not include plain language requirements in the matters upon which the Minister of Justice may publish regulations but s 40(1)(b)(iv) would permit the Information Regulator to research and report to Parliament upon the need for such measures.

[40] A Cavoukian, *Privacy by Design in Law, Policy and Practice A White Paper for Regulators, Decision-makers and Policy-makers* (Information and Privacy Commissioner, Ontario, Canada, 2011) at 10 states: 'It is equally important to examine very early in the planning process whether and how to limit the amount of personal data to the absolute minimum necessary.'

[41] Also see World Wide Web Consortium (W3C), *Web Application Privacy Best Practices W3C Working Group Note* (3 July 2012): 'Best Practice 9: Request the minimum number of data items at the minimum level of detail needed to provide a service … Best Practice 10: Retain the minimum amount of data at the minimum level of detail for the minimum amount of time needed. Consider potential misuses of retained data and possible countermeasures.'

[42] Electronic Frontier Foundation (EFF), *Mobile User Privacy Bill of Rights* (2012). 'Developers of mobile applications should only collect the minimum amount required to provide the service, with an eye towards ways to archive the functionality while anonymizing personal information.'

[43] e-Privacy Directive 2002/58/EC rec 30 provides: 'Systems for the provision of electronic communications networks and services should be designed to limit the amount of personal data necessary to a strict minimum...'. See further the discussion in European Data Protection Supervisor (EDPS), *Opinion 5/2018 Preliminary Opinion on Privacy by Design* (2018) at 8–9.

On the other hand, elsewhere the principle is limited to an assertion that the collection and use of personal information is limited only by the uses disclosed to or reasonably anticipated by the user.[44]

Neither of these positions reflect how the minimality principle is articulated in POPIA and GDPR. Minimality goes beyond the procedural requirements of notice and consent, and imposes a substantive restriction of lawfulness and reasonableness upon the purposes for which information can be processed.[45] Processing must be adequate, relevant and not excessive in relation to the purpose for which it is processed.[46] The purpose for which it is processed must be specific, explicitly defined, and lawful.[47] All processing is subject to the overriding requirements of lawfulness (requiring compliance with all conditions of lawful processing) and reasonableness (such that the right to privacy is not infringed).[48]

The requirements of POPIA and GDOR align closely with industry guidance that requires a legitimate or lawful purpose (related to a function or activity of the responsible party). However, the guidelines for implementation vary considerably based on which framework for notice and consent is adopted.

For example, the GSM Association (GSMA) Mobile Privacy Principles state:

> *'Only the minimum personal information necessary to meet legitimate business purposes and to deliver, provision, maintain or develop applications and services should be collected and otherwise accessed and used. Personal information must not be kept for longer than is*

[44] US Govt. Information Infrastructure Task Force (IITF) Privacy Working Group, *Privacy and the National Information Infrastructure: Principles for Providing and Using Personal Information* (6 June 1995): 'Organizations that gather personal information should take reasonable steps to prevent improper disclosure or alteration of information collected, and should enable individuals to limit the use of their personal information if the intended use is incompatible with the reason for which the information was collected, or not disclosed in the notice provided by collectors.' Also see Future of Privacy Forum and Center for Democracy & Technology, 'Best Practices for Mobile Application Developers' (12 July 2012) <https://fpf.org/wp-content/uploads/Apps-Best-Practices-v-beta.pdf> accessed 28 February 2020 at 5: 'If you cannot clearly articulate to users a reason why you are collecting certain data, do not collect it.'

[45] Federal Trade Commission, *Privacy Online: A Report to Congress* (1998) (at 49 note 28). By contrast collection limitation is enshrined in the Privacy Act of 1974 and requires federal agencies to collect only information that is 'relevant and necessary to accomplish a lawful purpose'.

[46] POPIA s 10. Cf GDPR art 5(1)(c).

[47] Ibid s 13(1). Cf GDPR art 5(1)(b).

[48] Ibid s 9. Cf GDPR which requires processing to be lawful and fair, and at several points reiterates that processing is restricted by the overriding fundamental rights and freedoms of the data subject.

necessary for those legitimate business purposes or to meet legal obligations and should subsequently be deleted or rendered anonymous."[49]

The GSMA 2012 guide to the implementation of PbD in the mobile ecosystem provides that all 'secondary' uses of data must be disclosed and require 'active' (that is, opt-in) consent.[50]

By contrast, other guides are based upon notice and opt-out consent, but even then they differ as to the modality for presenting notice. The Network Advertising Initiative (NAI) suggests the use of a 'layered' approach to the collection of opt-in consent using a just-in-time 'short' notice that alerts the user to the categories of third parties with whom the information may be shared, and a comprehensive privacy policy which provides fuller detail. An opt-out mechanism for cookies and non-cookie technologies must be subject to verification by the NAI compliance team.[51] The Interactive Advertising Bureau (IAB) guidance, on the other hand, suggests that it suffices to obtain permission to access data where required by the OS, and to provide disclosures in the privacy policy with an opt-out mechanism.[52] There is very little guidance on how to give notice about how anonymised data might be used for 'big data' analysis.[53]

Flowing from this analysis, recommendations are discussed below to strengthen the implementation of a PbD approach in the mobile ecosystem in South Africa through further research on the development of guidelines for the modalities of notice and consent, and the anonymisation and pseudonymisation of personal information (including clearer provisions on storage limitations when it is intended to use data for statistical and big data analysis).

---

[49] GSM Association (GSMA), *Mobile Privacy Principles: Promoting Consumer Privacy in the Mobile Ecosystem* (January 2011) at 5. The GSMA represents over 800 mobile network operators (carriers), but has broader reach to over 250 associated companies in the mobile ecosystem include device manufactures and OS providers.

[50] GSM Association (GSMA), *Privacy Design Guidelines for Mobile Application Development* (February 2012) at 4.

[51] Network Advertising Initiative (NAI), 'The NAI Code of Conduct' (2020) <https://www.networkadvertising.org/code-enforcement/code> accessed 2 March 2020, Network Advertising Initiative (NAI), *2015 Update to the NAI Mobile Application Code* (2015) and Network Advertising Initiative (NAI), *Guidance for NAI Members: Opt-In Consent* (November 2019).

[52] Interactive Advertising Bureau (IAB), *IAB Mobile Location Data Guide for Publishers* (New York, 2016). Also see Interactive Advertising Bureau (IAB), *IAB CCPA Compliance Framework for Publishers & Technology Companies (Draft for Public Comment)* (October 2019). Also see Digital Advertising Alliance, *DAA Ad Marker Implementation Guidelines for Mobile* (2014) and Digital Advertising Alliance, *Application of the DAA Principles of Transparency and Control to Data Used Across Devices* (2017).

[53] Michelle Finneran Dennedy, Jonathan Fox and Thomas R. Finneran, *The Privacy Engineer's Manifesto: Getting from Policy to Code to QA to Value* (Apress Open 2014) at 102.

(h) An Accountability Gap?

A larger issue focused on in this study is that none of the instruments studied deals comprehensively with accountability across the ecosystem. First, none of the instruments studied regulates 'upstream' technology and platform providers, save to the extent that they act as responsible parties by processing personal information in their own right.[54] There is thus no mechanism within the statutory framework of data protection laws to enforce the PbD requirement that technologies should be 'designed' for privacy from the outset, and liability may have to be founded in other areas of law.[55] As explained in chapter 2, design decisions made by app developers are constrained by the device hardware and OS, and informed by app store review policies and procedures.

Secondly, as regards 'downstream' processing, all the legislation deals in similar ways with the sub-contracting of specific processing functions (through a contract or mandate) to a processor (operator/service provider). However, sharing personal information with 'third parties' is not dealt with comprehensively or consistently. The term 'third party' is not defined in POPIA, but for the purposes of this analysis would include ad networks, content-sharing sites and social networking platforms. Such third parties typically collect one or more device identifiers for the purpose of linking that personal information to other personal information collected from the app (and combined with personal information collected from other sources), from which interests can be inferred for targeted advertising, 'friend' and content suggestions, and direct marketing (of their own products and services, or those of 'partner' organisations). Consent is collected for a specified purpose, and transfer to a third party must thus be explicitly disclosed. Fresh consent should be obtained when there is any material change in the collection, use or disclosure of personal information.[56]

However, some instruments provide that notice should be given before undertaking any further processing that is lawful on the grounds that it is 'compatible' with the

---

[54] For a recent analysis of Apple's potential liability as either a processor or joint controller under GDPR see Christian Kurtz and others, 'The Unlikely Siblings in the GDPR Family: A Techno-Legal Analysis of Major Platforms in the Diffusion of Personal Data in Service Ecosystems' in *Proceedings of the 52nd Hawaii International Conference on System Sciences* (Scholar Space, Grand Waile, Maui 8–11 January 2019).

[55] Data protection authorities can only encourage voluntary adoption of PbD by such parties, in the absence of an enforceable legal liability for data protection. For a discussion of how product liability law may inform the development of PbD see Ari Ezra Waldman, 'Privacy's Law of Design' (2018) 9 *UC Irvine L Rev* 1239.

[56] COPPA Rule 16 C.F.R §312 §312.5(a)(1). Implied in GDPR art 5(1)(b) and POPIA s 13(1) (purpose specification).

original purpose.[57] Notice should also be given before any transfer to third parties.[58] Further, in accordance with the PbD prescript to 'trust but verify',[59] some instruments require the responsible party to obtain assurances from the third party in relation to the lawfulness of its processing.[60] Recommendations are discussed below for the amendment of POPIA to introduce such provisions.

IV PROPOSED AMENDMENTS

In relation to the processing of information on terminal devices and the processing of electronic communication-related information such as traffic data and metadata, an amendment to the provisions of RICA should be considered. As the e-Privacy laws in Europe are currently undergoing an extensive, and controversial, revision, a detailed study of the e-Privacy Regulation and other relevant international and national guidelines is an important area of further research to determine the best approach to the content of any legislative amendments in South Africa.

It is recommended that the following amendments to POPIA should be adopted to address provisions which are not consistent with the conditions of lawful processing outlined in the Act, and with the PbD approach that those conditions imply:

1. Section 18(4)(a) should be deleted in its entirety. To permit a data subject to consent to non-compliance with the requirement for notice is nonsensical and inconsistent with the condition of openness and the basis for consent as being voluntary, specific and *informed*.

---

[57] GDPR art 13(3) & art 14(4). See below proposed amendment of POPIA.

[58] Ibid rec 61 provides: 'Where personal data can be legitimately disclosed to another recipient, the data subject should be informed when the personal data are first disclosed to the recipient. Where the controller intends to process the personal data for a purpose other than that for which they were collected, the controller should provide the data subject prior to that further processing with information on that other purpose and other necessary information. Where the origin of the personal data cannot be provided to the data subject because various sources have been used, general information should be provided.'

[59] This is in accordance with the principle of openness applied to the mobile applications ecosystem.
A Cavoukian and M Prosch, *The Roadmap for Privacy by Design in Mobile Communications: A Practical Tool For Developers, Service Providers, and Users* (Toronto, ON, Canada: Office of the Privacy Commissioner, Ontario, Canada, 2010) at 6.

[60] COPPA Rule 16 C.F.R §312.8 provides: 'The operator must also take reasonable steps to release children's personal information only to service providers and third parties who are capable of maintaining the confidentiality, security and integrity of such information, and who provide assurances that they will maintain the information in such a manner.' This goes beyond seeking contractual assurances and requires additional reasonable steps to verify that the third party does comply with such measures.

2. Section 18(4)(b) should be deleted in its entirety. The provision is inconsistent with the conditions of openness and data subject participation. The requirement that the data subject's legitimate interests (and, it must be added, their constitutional right to privacy) must not be prejudiced is encapsulated by the requirement for notice. Where section 18 provides a limited exception to the giving of notice, the provisions of section 18(4)(b) should apply (only to those exceptions) as a condition for invoking the exception.

3. Section 18(4)(d) and (e) are currently framed too broadly, and should be amended to restrict their application only to the situation where information is collected from a source other than the data subject, and to impose reasonable safeguards.[61] While consent is not required for processing pursuant to a legitimate interest of the responsible party, or for further processing that is compatible with the original purpose of collection, the condition of openness and the condition of data subject participation (including the effective exercise by the data subject of their rights to object to processing) cannot be implemented without notice of the collection, use and disclosure of information and the data subject's rights in relation to that processing.

   The proposed amendments would read as follows:

   '(d) [*In the case of personal information collected from a source other than the data subject*] compliance would ~~prejudice~~ [*render impossible or seriously impair the achievement of*] a lawful purpose of the collection [*, provided that reasonable measures are taken to safeguard the data subject's rights and legitimate interests*];'

   (e) [*In the case of personal information collected from a source other than the data subject*] compliance is ~~not reasonably practicable~~ [*impossible or would involve disproportionate effort*] in the circumstances of the particular case [*, provided that reasonable measures are taken to safeguard the data subject's rights and legitimate interests*];'

4. Section 18(4)(f) should be deleted in its entirety. It is inconsistent with the definition of processing (which includes collection) to exempt notice where information is collected in personally identifiable form. Furthermore, it is inconsistent with the

[61] Cf GDPR art 14(5)(b).

conditions of openness, data subject participation and security to permit such a widely-framed exception. If the provision is deleted, a responsible party who collects personal information would have to explain if the personal information will be de-identified after it is collected, and what other measures would be taken to ensure the security, integrity and confidentiality of the information, such as pseudonymisation, and encryption of data in transit and in storage. The responsible party would be exempt from further compliance with POPIA in respect of de-identified data *after* it has been de-identified.[62] Data subjects will enjoy the autonomy and control over their own personal information inherent in the right to privacy and the conditions of openness and data subject participation only if they are informed and thus free to choose whether their personal information may be de-identified and used in an anonymous form. Persons who do not collect identifying information at all remain exempt from POPIA,[63] although best practice may be that they should still provide a clear statement to data subjects that they do not collect personal information (if, for example, all processing of personal information stays on the user's device, that should be explained).

5. Section 18 should be amended by the insertion of a new section 18(1A)[64] to read:

'*Where the responsible party intends to further process the personal information for a purpose other than that for which it was originally collected, the responsible party shall provide the data subject with information on that further purpose. For the purpose of this section, a transfer of personal information to a third party (whether or not that personal information has been de-identified or not) shall be regarded as further processing*.'

A consequential amendment to section 18(2) is required as follows:

'The steps referred to in subsection[*s*] (1) [*and 1(A)*] must be taken–

(a) if the personal information is collected directly from the data subject, before the information is collected, [*and before any further processing*], unless the data subject is already aware of the information referred to in that subsection; or

[62] POPIA s 5(1)(b).
[63] Ibid s 1 definition of 'personal information'.
[64] Cf GDPR art 13(3) and art 14(4).

(b) in any other case, before the information is collected or as soon as reasonably practicable after it has been collected [, *and before any further processing*].'

The purpose of this insertion would be to make the conditions of openness and data subject participation more effective in those instances where the data subject may not reasonably have anticipated the processing at the time of collection. It is further intended to complement section 18(3), which limits the requirement of fresh notice to situations where new types of personal information are collected, or the purpose of processing changes.

6. To address the current lacunae in relation to accountability, a new section 21A should be inserted to provide that a responsible party can transfer personal information to a third party only with an assurance from that third party that the personal information will be processed lawfully.[65] The term 'third party' should be defined, and should include anyone who processes information as an operator on behalf of the responsible party and for their own further purposes. A responsible party can protect themselves by insisting that an operator, such as a back-end service provider, agrees to process personal information solely for the purposes contained in their contract with the responsible party. If a responsible party chooses to appoint an operator without insisting on this safeguard, then it must take the additional reasonable measures required by the proposed amendment to satisfy itself that there is an assurance that the personal information will be processed lawfully.

   Further, the situations where the third party is a joint responsible party should be clarified and the statute should impose joint and several liability on both responsible parties in those situations. A policy decision must be taken as to whether processing by a third party that confers a benefit on the original responsible party (for example, through advertising revenue) should be regarded as joint processing. It is suggested that this would be going too far. It is sufficient that at present under POPIA a third party, such as an advertising network or social media platform, is a responsible party in their own right in respect of all processing of personal information (for the means and purposes of processing they determine).[66] They are required to give notice as

[65] Cf COPPA Rule 16 C.F.R §312.8.
[66] POPIA s 1 definition of 'responsible party'. This has the same effect as the definition of 'controller' under GDPR. There is thus no need for a deeming provision such as that included under COPPA Rule 16 C.F.R §312.2

soon as reasonably possible after collection of the personal information, save to the extent that the data subject has already been made aware of who they are, what personal information they receive, and what purposes they process it for (e.g. through an sufficiently detailed disclosure in a partner mobile app privacy policy). The mobile app developer would be in breach of POPIA if they transferred personal information to any third party without appropriate assurances, but would not be jointly liable for any further breaches committed by that third party.

in terms of which a person who directly benefits from receiving personal information is deemed to be an operator even though they have not collected the personal information.

The proposed insertion would read:

'<u>Lawful processing of personal information by third party</u>

21A. (1) For the purpose of this section the term 'third party' means a person who processes personal information received from a responsible party, including an operator to the extent that they process the personal information for any purpose other than the purposes authorised by the responsible party in terms of a written contract between the responsible party and the operator.

(2) A responsible party shall not transfer personal information to a third party unless the third party has provided an assurance that they will process the information lawfully, which must include an assurance that they will be capable of establishing and maintaining the security measures referred to in section 19.

(3) Responsible parties will be jointly liable for any breach of this Act to the extent that they jointly determined the means and purposes of processing. A responsible party will not be regarded as jointly liable for the purposes of this provision if it merely benefited (directly or indirectly) from the processing by a third party to whom it transferred personal information, save to the extent that it failed to comply with subsection 2.'

7. The accountability gap identified in relation to upstream technology and platform providers requires further investigation, and consultation with industry stakeholders and other data protection supervisory authorities, to determine the best means of requiring such parties to take PbD principles into consideration and design products, services and applications that make it possible for responsible parties and operators to comply with POPIA.[67] Currently, such parties are liable as responsible parties to the extent that they process personal information.[68] As there is no precedent for introducing a direct statutory liability beyond this,[69] to suggest an amendment of POPIA would be premature and would place South Africa out of step with international practice, contrary to the stated intention of section 2 of POPIA.

[67] Cf GDPR rec 78.
[68] POPIA s 1 definition of 'responsible party'. An area for further research is the extent to which product liability or delictual liability could be applied.
[69] Cf discussion in chapter 4 on the statement of the FTC in relation to the 2013 amendment of the definition of 'operator' under COPPA expressly disavowing that it was intended to apply to app stores.

However, as discussed in chapters 7 and 8, industry standards may in any event play a more useful role in addressing sector-specific technical requirements, and the Information Regulator is empowered to consult widely and promote such measures in conjunction with other relevant government departments[70] and industry stakeholders.

V RECOMMENDATIONS FOR FUTURE RESEARCH

Although POPIA provides a strong framework for data protection, and is consistent with the PbD approach, there are further issues it does not address adequately. First, best practice guidelines indicate that privacy policies and disclosure notices must be prominently posted, readily accessible, and carefully drafted to ensure that they are clear and easy to understand, in relation to both layout and language. While the Consumer Protection Act[71] provides some guidelines, comprehensive guidance to mobile app developers should be drafted. That guidance should take into account the requirements referred to above in the CCPA, COPPA, CalOPPA and GDPR, both insofar as those statutes may apply directly to South African app developers, and insofar as they are the latest general international guidelines to which due regard is to be paid by the Information Regulator in the performance of its functions and exercise of its powers.[72]

Secondly, that guidance must consider the best practice guidelines issued by other national supervisory authorities to mobile application developers indicating that a 'layered' approach should be used. Disclosure should be set out in a clear, comprehensive privacy policy, but in addition, short 'just-in-time' notices delivered in context (that is, just before the information is collected) should be given for collection, use or disclosure practices that are unrelated to the app's function and may surprise the user. [73] This does not require all disclosure to take place in this manner, and in fact, to do so might be intrusive and do more

[70] Principally the Department of Communications, but also in relation to mobile app developers in the SMME sector, the Department of Small Business Development.
[71] CPA.
[72] POPIA s 44(1)(d).
[73] See State of California Office of the Attorney General, *Privacy on the Go: Recommendations for the Mobile Ecosystem* (2013) at 12. Also see the FTC reports referred to in chapter 4, and National Telecommunications and Information Administration (NTIA) US Department of Commerce, *Short Form Notice Code of Conduct to Promote Transparency In Mobile App Practices* (2013 July 25).

harm than good by overwhelming the user.[74] Short targeted notices could be combined with periodic reminders to users on how they can configure their privacy preferences.[75]

Thirdly, industry guidance should be developed not only on technical standards for encryption and security of personal information, but also for the de-identification (anonymisation) and pseudonymisation of personal information and the statistical and big data analysis techniques applied in app analytics. This may warrant an amendment to POPIA to introduce an express requirement that if the purpose of processing can be achieved by de-identifying the information, it must be de-identified as soon as reasonably possible.[76]

As there are limits to the detail in which these objectives can be addressed in a general statute, sector-specific codes of conduct, such as those referred to in relation to the online advertising industry in the discussion in chapter 6, should provide additional guidance,[77] particularly in relation to the use of icons, privacy seals/trust marks and other technical (default) settings that should be used to manage data protection in that context. Consumer testing to identify the modalities and language that promote the clearest understanding among South African data subjects is an important area for research, which may inform the development of evidence-based assessment criteria for the approval of industry codes of conduct.

In addition, the Information Regulator is empowered to provide educational advice to the public, as well as to industry participants, on matters relevant to the protection of personal information.[78] The development of a consumer data protection portal[79] and a mobile

---

[74] GDPR art 13(1) requires notice to be given 'at the time when personal data are obtained' but rec 32 records that the request must be 'clear, concise and not unnecessarily disruptive'.
[75] E.g. Facebook's "privacy checkup" tool.
[76] POPIA s 14(4) currently provides that a responsible party must destroy, delete or de-identify a record of personal information as soon as reasonably practicable after the responsible party is no longer authorised to retain the record. However s 14(1) permits retention on wide grounds including where the data subject has consented. Arguably it should not be possible to request consent to retain information in an identifiable form when this is not required by for the purpose for which it is being retained.
[77] Ibid s 50(1) empowers the Information Regulate to issue a code of conduct. In terms of section 61 it may do so either on its own initiative (but after consultation with affected stakeholders or representative bodies) or on application by any body sufficiently representing (in the opinion of the regulator) the industry, profession or vocation that will be regulated by the code. The application must be made in the prescribed form, being Form 3 of the Regulations relating to the Protection of Personal Information in R 1383 *GG* 42110 of 14 December 2018.
[78] POPIA s 40(1)(a).
[79] E.g. as indicated in chapter 4 the FTC has developed a children's privacy portal providing parents with user-friendly information. FTC consent orders have included a requirement that the operator of the website or online service include a prominent notice and link to the portal on their website or service homepage.

application developer's guide to implementing PbD in compliance with POPIA[80] would be promising areas for practical application research.

Further, the Information Regulator is empowered to monitor compliance, conduct research and issue reports, including reports and recommendations upon the use of unique identifiers of data subjects.[81] As noted in chapter 2 from a review of previous studies, this is an area where there is very little transparency, but a high risk of privacy invasion when profiling of individuals is used for purposes that could have legal or other significant effects. However, as shown in the comparative conclusions at the beginning of this chapter, there remains a lack of clarity and consistency with regard to the treatment of online identifiers in the statutes considered. This is accordingly an area requiring further in-depth multi-disciplinary empirical research.

In relation to children, COPPA and GDPR require *verified* parental consent.[82] As POPIA already also requires that consent must be given by a competent person, such as the parent of a child, it is implied that the responsible party must be able to prove that the consent was given by the parent and not by the child or an incompetent person (that is, a person who is not a holder of parental authority). However, in an online environment, this may prove difficult, and additional regulatory guidance on what measures should be adopted appear to be needed. This is not an issue upon which the Minister of Justice is empowered to issue regulations under section 112, and therefore it appears to be a matter for assessment of existing practices,[83] consultation and cooperation in international "privacy sweeps" of child-directed apps,[84] and a report to Parliament on any legislative amendment or administrative action required.[85]

---

[80] See the guidance documents referred to in chapter 4. As noted in that chapter, clear cross-referencing to statutory obligations and interpretation notes should be given where possible.
[81] POPIA s 40(1)(b)(vii).
[82] COPPA Rule 16 C.F.R §312 §312.5(a)(1) and GDPR art 8(2).
[83] POPIA s 89 – although these powers relate only to a particular instance of processing the Information Regulator is empowered to act on its own initiative. It might usefully undertake a 'privacy sweep' of children's apps in the most popular app marketplaces in South Africa as other supervisory authorities have done. See Federal Trade Commission, *Mobile Apps for Kids: Current Privacy Disclosures are Disappointing* (February 2012), Federal Trade Commission, *Mobile Apps for Kids: Disclosures Still Not Making the Grade* (December 2012).
[84] POPIA s 40(1)(c)(ii). E.g. The Global Privacy Enforcement Network (GPEN) was established in terms of OECD, *Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy* (2007). Members (South Africa is not presently a member) conduct an annual 'privacy sweep'. See Lauren Newton, 'GPEN Sweep 2018 - International investigation finds that organisations should be doing more to achieve privacy accountability' (*Global Privacy Enforcement Network*,, 5 March 2019) <https://privacyenforcement.net/press-releases> accessed 04 April 2020.
[85] POPIA s 40(1)(b)(iv).

Last, this dissertation has not undertaken a comprehensive comparison of data subject rights or the issue of transborder flows of information. Legal studies that consider these issues in depth or multi-disciplinary studies that address the modalities of implementing and enforcing compliance with the legal provisions in a particular technology would usefully contribute to a stronger data protection framework in South Africa.

VI CONCLUDING REMARKS

Caution should be exercised in relation to observations that PbD is a new legal requirement, for from its original conception to its current applications it has been a transdisciplinary concept born from a recognition of the limitations of regulation to achieve adequate protection of privacy. The end-goal of PbD is that privacy is embedded as the default setting in the design of technological products. In other words, it must be expressed in the digital code as well as in the legal code.[86]

The explicit introduction of PbD as a legal requirement for controllers under GDPR was intended to 'strengthen' the PbD approach that was already implicit in the 1995 Directive.[87] On analysis, no new data-processing principle has been added by the article itself,[88] or by the other additions and amendments to GDPR, that is not contained in POPIA. However, amendments are proposed to the notice and accountability provisions, drawn from comparative analysis of US and EU law, in order to enhance openness, data subject participation and to address (in part) the accountability gap described in this study.

While an expressly stated legal obligation to implement PbD may be an important 'conversation starter' and act as a red flag raising public and industry awareness of

---

[86] Giorgia Bincoletto, 'A Data Protection by Design Model for Privacy Management in Electronic Health Records' in *Annual Privacy Forum: Privacy Technologies and Policy* (Springer, Rome, Italy 13–14 June 2019) at 163; Aurelia Tamò-Larrieux, *Designing for Privacy and its Legal Framework –Data Protection by Design and Default for the Internet of Things* (Springer 2018).

[87] Data Protection Directive 95/46/EC.

[88] Lee A Bygrave, 'Data Protection by Design and by Default: Deciphering the EU's Legislative Requirements' (2017) 4 *Oslo Law Review* 105–120. Although the author welcomes art 25 as potentially strengthening data protection in Europe, he identifies a number of flaws that may hinder successful implementation. While he regards it as a moot point whether art 25 adds new data protection principles, his reasoning supports the argument advanced in this chapter that the data protection principles upon which PbD rests are 'adequately' set out in the legislation, and enforcement of a PbD approach must be implemented at the level of secondary regulatory measures. The author states: 'Whether Article 25 embraces other data protection principles than those listed in Article 5 is a moot point and arguably of academic interest only, as the pith of such principles is adequately covered by Article 5, at least at an operational level. Further guidance on the parameters of Article 25 measures is expected to come from codes of conduct prepared by industry bodies (Article 40(2)(h)), from certification schemes (Article 25(3) in combination with Article 42), and from advice provided by data protection authorities'.

privacy as a priority,[89] such a provision will never be sufficient to achieve a PbD outcome. What is required is specific, enforceable legal obligations, complemented by detailed sector-specific guidance, to set harmonised standards and methodologies. That can be worked out only in co-operative, intensive dialogue between regulators and industry stakeholders.[90] In particular, those who design the technologies and platforms on which mobile apps are built and marketed must be brought within the legal accountability framework. Without such measures, a general legal duty imposed on app developers (as responsible parties) is all but unenforceable, and worse, if it is set out in a vague formulation contained within a complex and fragmentary legal framework, it may actually hinder the protection of information privacy rather than promote its protection.

[89] European Data Protection Supervisor (EDPS), *Opinion 5/2018 Preliminary Opinion on Privacy by Design* at 17. The report also notes that political attention to tracking and profiling is also playing a role in increasing awareness.

[90] Article 29 Data Protection Working Party and Working Party on Police and Justice, *The Future of Privacy: Joint Contribution to the Consultation of the European Commission on the Legal Framework for the Fundamental Right to Protection of Personal Data* (WP168) at 14.

TABLE OF LEGISLATION

INTERNATIONAL INSTRUMENTS

UNITED NATIONS

Universal Declaration of Human Rights (adopted 10 December 1948 UNGA Res 217 A(III)

International Covenant on Civil and Political Rights (adopted 16 December 1966, entered into force 23 March 1976) 999 UNTS 171

AFRICA

African Union Convention on Cyber Security and Personal Data Protection (Malabo, 2014)

Economic Community of West African States (ECOWAS) Supplementary Act on Personal Data Protection within ECOWAS (Abuja, 2010)

COUNCIL OF EUROPE

Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights, as amended) (ECHR) ETS 5, 213 UNTS 221

Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (COE Convention) ETS 108 (1981, as amended in 1999)

Council of Europe Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding supervisory authorities and transborder data flows (entry into force 1 July 2004) ETS 181 (2001)

Council of Europe Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, CETS 223 (2018)

EUROPEAN UNION

Charter of Fundamental Rights of The European Union (2000/C 364/01)

Treaty on the Functioning of the European Union (TFEU) (Treaty of Lisbon) (13 December 2007)

UNITED STATES

Federal Legislation

Federal Laws

Airline Deregulation Act of 1978, 49 U.S.C. § 1371 (2018)

Algorithmic Accountability Act of 2019 S.1108 116th Congress (2019-2020)

American Data Dissemination Act of 2019 S.142 — 116th Congress (2019-2020)

Cable Communications Policy Act of 1984, 47 U.S.C. § 551 (2018)

Children's Online Privacy Protection Act of 1998, 15 U.S.C. §§ 6501 - 6506 (2018) (COPPA)

Communications Act of 1934, as amended by, Telecommunications Act of 1996, 47 U.S.C. § 222 (2018)

Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM) Act of 2003, Pub.L. 108-187 Stat.2699 15 U.S.C. § 7701 et seq.

Customer Online Notification for Stopping Edge-provider Network Transgressions (CONSENT) Act 115 Con. 2nd session

Designing Accounting Safeguards To Help Broaden Oversight and Regulations on Data (DASHBOARD) Act S.1951 — 116th Congress (2019-2020)

District Courts Jurisdiction, 28 U.S.C. §§ 1330-1369 (2018)

E-Government Act of 2002, Pub Law 107–347, 116 Stat. 2899

Electronic Communications Privacy Act of 1986, 18 U.S.C. §§ 2510 (2018) (ECPA)

Fair Credit Reporting Act of 1970, 15 U.S.C. § 1681 (2018) (FCRA)

Family Educational Rights and Privacy Act of 1974, 20 U.S.C. § 1232g; 34 C.F.R. §§ 99.1 – 99.8 (FERPA)

Federal Information Security Modernization Act of 2014, Pub.L. No. 113–283, 128 Stat. 3073 (FISMA)

Federal Trade Commission Act of 1914, 15 U.S.C. §§ 41–58 (2018) (FTCA)

Financial Services Regulatory Relief Act, Pub Law 109-351, 120 Stat. 1966-2010

Fixing America's Surface Transportation (FAST) Act of 2015, Pub. L. No. 114-94 (FAST Act)

Foreign Intelligence Surveillance Act of 1978, 50 U.S.C. §§ 1801–1885c (2018) (FISA)

Freedom of Information Act of 1966, 5 U.S.C. § 552 (2018) (FOIA, US)

Gramm-Leach-Bliley Act of 1999, Pub.L. No. 106–102, 113 Stat. 1338 (GLBA)

Health Information Technology for Economic and Clinical Health (HITECH) Act, Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009 (ARRA), Pub. L. No. 111-5, 123 Stat. 226 (HITECH Act)

Health Insurance Portability and Accountability Act of 1996, Pub.L. No. 104–191, 110 Stat. 1936 (HIPAA)

Privacy Act of 1974, 5 U.S.C. § 552a (2018)

Regulatory Flexibility Act of 1980, 5 U.S.C. §601–612 (2018)

Right to Financial Privacy Act of 1978, 12 U.S.C. §§ 3401 (2018)

Social Media Privacy Protection and Consumer Rights Act of 2019 S.189 116th Congress (2019-2020)

Stored Communications Act of 1986, 18 U.S.C. §§ 2701 - 2712 (2018)

Telephone Consumer Protection Act of 1991 (TCPA) 47 U.S.C. § 227

Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (Wiretap Act) Pub. L. 90-351 34 U.S.C. §10101

Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, Pub.L. 107–56, 115 Stat. 272 (USA Patriot Act)

USA Freedom Act of 2015, Pub Law No. 114-23, 129 Stat. 268 (2015)

Video Privacy Protection Act of 1988, 18 U.S.C. § 2710 (2018)

Federal Regulations

Children's Online Privacy Protection Rule, 16 C.F.R part 312 (COPPA Rule)

FTC Privacy of Consumer Financial Information Rule, 16 C.F.R part 313 (2019)

HIPAA Privacy Rule, 45 C.F.R. parts 160 & 164 (A) & (E) (2018)

HIPAA Security Rule, 45 C.F.R. parts160 and 164 (A) & (C) (2018)

Privacy of Consumer Financial Information (Regulation P), 12 C.F.R. part 1016 (2020)

Standards for Safeguarding Customer Information, 16 C.F.R. § 314

Draft Bills

Consumer Online Privacy Rights Act, S.B. 2968, 116th Congress, 1st session (2019)

Data Care Act of 2018 S.3744 — 115th Congress

US Consumer Data Privacy Act of 2019 (discussion draft) available at https://aboutblaw.com/NaZ, accessed on 25 February 2020

Draft Regulations

Children’s Online Privacy Protection Rule: Final Rule Amendments, FR 79(12) Part II (17 January 2013)

Privacy of Consumer Financial Information Rule Under the Gramm-Leach-Bliley Act: A Proposed Rule by the Federal Trade Commission, 84 FR 13150 (22 February 2020)

Request for Public Comment on the Federal Trade Commission’s Implementation of the Children’s Online Privacy Protection Rule, FR 84(143) (25 July 2019)

STATE OF CALIFORNIA

Laws

Bill to amend §22575 of Cal. Bus. & Prof. Code, A.B. 370, 2013-2014, ch.390, 2013, Cal. Stat. (effective 1 January 2014)

California Constitution

California Consumer Privacy Act of 2018, Cal. Civ. Code §§ 1798.100 - 1798.199 (CCPA)

California Electronic Communications Privacy Act of 2015, Cal. Pen. Code §1546 (CalECPA)

Enforcement, Cal. Bus. & Prof. Code §§17200-17210

Online Privacy Protection Act of 2003, Cal. Bus. & Prof. Code §§ 22575-22579 (2004)

EUROPEAN UNION

European Union Laws

Commission Regulation (EU) no 611/2013 of 24 June 2013 on the measures applicable to the notification of personal data breaches under Directive 2002/58/EC of the European Parliament and of the Council on privacy and electronic communications OJ L 173, 26.6.2013

Commission Decision (EU) no 2004/915/EC of 27 December 2004 amending Decision 2001/497/EC as regards the introduction of an alternative set of standard contractual clauses for the transfer of personal data to third countries (notified under document number C(2004) 5271) (Text with EEA relevance) OJ L 385, 29.12.2004Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts OJ L 95, 21.4.1993

Council Directive 93/104/EC of 23 November 1993 concerning certain aspects of the organization of working time OJ L 307, 13.12.1993

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (Data Protection Directive) OJ 1995 L 281/31, 23.11.1995

Directive 98/34/EC of the European Parliament and of the Council of 22 June 1998 laying down a procedure for the provision of information in the field of technical standards and regulations OJ L 204, 21.7.1998 (repealed 6 October 2015)

Directive 1999/5/EC of the European Parliament and of the Council of 9 March 1999 on radio equipment and telecommunications terminal equipment and the mutual recognition of their conformity OJ L 91/10, 7.4.1999

Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on Electronic Commerce) OJ L 178/1, 17.7.2000

Directive 2002/19/EC of the European Parliament and of the Council of 7 March 2002 on access to, and interconnection of, electronic communications networks and associated facilitie(Access Directive), OJ L 108, 24.4.2002

Directive 2002/20/EC of the European Parliament and of the Council of 7 March 2002 on the authorisation of electronic communications networks and services (Authorisation Directive) OJ L 108, 24.4.2002

Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive) OJ L 108, 24.4.2002

Directive 2002/22/EC of the European Parliament and of the Council of 7 March 2002 on universal service and users' rights relating to electronic communications networks and services (Universal Service Directive) OJ L 108, 24.4.2002

Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC OJ L105, 13.04.2006.

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector 2002/58/EC (e-Privacy Directive) OJ L 201/37, 31.7.2002

Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) no 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws OJ L 337, 18.12.2009

Directive 2014/53/EU of the European Parliament and of the Council of 16 April 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of radio equipment and repealing Directive 1999/5/EC OJ L 153/62, 22.5.2014 (RE-Directive)

Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services OJ L 241, 17.9.2015

Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA OJ L 119, 4.5.2016 (EU General Data Protection Regulation; GDPR)

Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing The European Electronic Communications Code (Recast) OJ L 321, 17.12.20d18 (EECC)

Draft Commission Implenting Decision (EU) on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council Ref: Ares(2020)6654686, 12.11.2020 Proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) Brussels, 25.1.2012 COM(2012) 11 final 2012/0011 (COD)

Proposal for a regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) Brussels, 10.1.2017 COM(2017) 10 final 2017/0003 (COD)

Regulation (EC) No 1211/2009 of the European Parliament and of the Council of 25 November 2009 establishing the Body of European Regulators for Electronic Communications (BEREC) and the Office, OJ L 337, 18.12.2009

Regulation (EU) 2015/2120 of the European Parliament and of the Council of 25 November 2015 laying down measures concerning open internet access and amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services and Regulation (EU) No 531/2012 on roaming on public mobile communications networks within the Union, OJ L 310, 26.11.2015

Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data

by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (Text with EEA relevance.) PE/31/2018/REV/1. OJ L 295, 21.11.2018

BELGIUM

Loi du 13 juin 2005 relative aux communications électroniques (Law of 13 June 2005 on electronic communications) (Moniteur belge, 20 June 2005, p. 28070)

GERMANY

Telekommunikationsgesetz (Law on Telecommunications) of 22 June 2004 (BGBl. 2004 I, p. 1190)

UNITED KINGDOM

Data Protection Act 1984 (c. 35)

Data Protection Act 2018 (c.12)

SOUTH AFRICA

Legislation

Children's Act 38 of 2005

Companies Act 71 of 2008

Constitution of the Republic of South Africa, 1996

Consumer Protection Act 68 of 2008 (CPA)

Copyright Act 98 of 1978

Designs Act 195 of 1993

Electronic Communications Act 36 of 2005 (ECA)

Electronic Communications and Transactions Act 25 of 2002 (ECTA)

National Small Enterprise Act 102 of 1996

Promotion of Access to Information Act 2 of 2000 (PAIA)

Protection of Personal Information Act 4 of 2013 (POPIA)

Protection, Promotion, Development and Management of Indigenous Knowledge Act 6 of 2019

Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 of 2002 (RICA)

Trade Marks Act 194 of 1993

Regulations

Commencement of section 1, part A of chapter 5 and sections 112 and 113 of The Protection of Personal Information Act, 2013 (Act no. 4 of 2013), Proc R 25 GG 37544 of 11 April 2014

Commencement of certain sections of the Protection of Personal Information Act, Proc R 21 GG 43461 of 22 June 2020

Determination of threshold in terms of the Consumer Protection Act, 2008 (Act no. 68 of 2008) in GN 294 GG 34181 of 1 April 2011

Explanatory memorandum on the objects of the Protection of Personal Information Bill, published in GG 32495 of 14 August 2009

Promotion of Access to Information Act, 2000 (Act 2 of 2000) Exemption of Certain Private Bodies from Compiling Manual in GN 1222 GG 39504 of 11 December 2015

Regulations relating to the Protection of Personal Information in R 1383 GG 42110 of 14 December 2018

AUSTRALIA

Privacy Act 1988 (Cth)

CANADA

Personal Information Protection and Electronic Documents Act S.C. 2000, c.5 (PIPEDA)

HONG KONG

Personal Data (Privacy) Ordinance, Laws of Hong Kong (Cap 486) (PDPO)

TABLE OF CASES

SOUTH AFRICA

Decided Cases

Afrox Healthcare Bpk v Strydom 2002 (6) SA 21 (SCA)

Baleni and Others v Minister of Mineral Resources and Others 2019 (2) SA 453 (GP)

Barkhuizen v Napier 2007 (5) SA 323 (CC)

Bernstein and others v Bester and others NNO 1996 (2) SA 751 (CC)

Beukes v Smith 2020 (4) SA 51 (SCA)

BOE Bank Bpk v Van Zyl 2002 5 SA 165 (C)

Brink v Humphries & Jewell (Pty) Ltd 2005 (2) SA 419 (SCA)

Brisley v Drotsky 2002 (4) SA 1 (SCA)

Broude v McIntosh and Others 1998 (3) SA 60 (SCA)

Castell v De Greef 1994 (4) SA 408 (C)

Children's Resource Centre v Pioneer Food 2013 (2) SA 213(SCA)

De Pass v The Colonial Govt (1886) 4 SC 283

Eerste Nasionale Bank van Suidelike-Afrika Bpk v Saayman NO 1997 (4) SA 302 (SCA)

Everfresh Market Virginia (Pty) Ltd v Shoprite Checkers (Pty) Ltd 2012 (1) SA 256 (CC)

Financial Mail (Pty) Ltd v Sage Holdings Ltd and Another 1993 (2) SA 451 (A)

H v W 2013 (2) SA 530 (GSJ)

Hohne v Super Stone Mining (Pty) Ltd 2017 (3) SA 45 (SCA)

Isparta v Richter and Another 2013 (6) SA 529 (GNP)

Keens Group Co (Pty) Ltd v Lötter 1989 (1) SA 585 (C)

Khumalo and others v Holomisa 2002 (5) SA 401 (CC)

Louwrens v Oldwage 2006 (2) SA 161 (SCA)

Makate v Vodacom (Pty) Ltd 2016 (4) SA 121 (CC)

Medscheme Holdings (Pty) Ltd and another v Bhamjee 2005 (5) SA 339 (SCA)

Mighty Solutions CC t/a Orlando Service Station v Engen Petroleum Ltd and another 2016 (1) SA 621 (CC)

Natal Joint Municipal Pension Fund v Endumeni Municipality 2012 (4) SA 593 (SCA)

National Media Ltd and another v Jooste 1996 (3) SA 262 (A)

Nationwide Airlines (Pty) Ltd (in Liquidation) v South African Airways (Pty) Ltd 2016 (6) SA 19(GJ)

NM and others v Smith and others (Freedom of Expression Institute as amicus curiae) 2007 (5) SA 250 (CC)

O'Keeffe v Argus Printing and Publishing Co Ltd and another 1954 (3) SA 244 (C)

Royal Canin South Africa (Pty) Ltd v Cooper and another 2008 (6) SA 644 (SE)

S v A and another 1971 (2) SA 293 (T)

SA Sentrale Ko-op Graanmaatskappy Beperk v Shifren en andere 1964 (4) SA 760 (A)

Santam Insurance Co Ltd v Vorster 1973 (4) SA 764 (A)

Seetal v Pravitha and Another NO 1983 (3) SA 827 (D)

South African Railways and Harbours v Cemafrique (Pty) Ltd 1978 (3) SA 388 (A)

Spenmac (Pty) Ltd v Tatrim CC 2015 (3) SA 46 (SCA)

Spindrifter (Pty) Ltd v Lester Donovan (Pty) Ltd 1986 (1) SA 303 (A)

Waring & Gillow Ltd v Sherborne 1904 TS 340

UNITED STATES

Decided Cases

American Postal Workers Union v United States Postal Service 595 FSupp 1352 (DDC 1984)

Boyd v United States 116 U S 616, 630 (1886)

Carpenter v United States 585 US (2018)

Central Hudson Gas & Electric Corp. v Public Service Commission 447 US 557 (1980)

Dun & Bradstreet Inc. v Greenmoss Builders Inc. 472 US 749 (1985)

Gelbard v United States 408 US 41 (1972)

Harris v Delta Airlines Inc 247 CalApp4th 884 (2016)

In re Equifax Inc. customer data security breach litigation 362 F Supp 3d 1295 (ND Ga 2019)

In re Google Inc. Cookie Placement Consumer Privacy Litigation No 17-1480 (3d Cir opinion 6 August 2019)

In re Google Inc. Cookie Placement Consumer Privacy Litigation 806 F3d 125 (3d Cir 2015)

In re Pharmatrak 329 F3d 9, 15, 18-19 (1st Cir2003)

In re Zynga Privacy Litigation 750 F3d 1098, 1105-06 (9th Cir 2014)

National Organization for Marriage v Daluz 654 F3d 115, 121 (1st Cir 2011)

Oracle America Inc. v Google Inc. 886 F3d 1179 (Fed Cir 2018)

Sedwick Claims Management Services v Barrett Business Services Inc 2007 WL 1053303 (D Or 2007)

United States v Carpenter 819 F3d 880 (6th Cir 2016)

United States v Jones 565 US 400 (2012)

United States v Miller 425 US 435 (1976)

Class Action Law Suits

Farag et al v Kiip Inc. No 2019 CH 01695 (Ill Cir Ct Cook Cnty Oct 18, 2019) (settlement order)

In re Carrier IQ, Inc. Consumer Privacy Litigation Case No 12-md-02330 EMC (NC) (ND Cal Sep 27, 2013)

Robert Cullen, individually and on behalf of all others v Zoom Video Communications Inc. Case No 5:20-cv-02155 (ND Cal, Mar 30, 2020)

Vasil v Kiip Inc. No 16-CV-09937 (ND Ill Mar 5, 2018)

Federal Trade Commission Enforcement Actions

Federal Trade Commission v Frostwire LLC and Angel Leon Case No 111-cv-23643 (SD Fla Oct 12, 2011) (injunction)

FTC v ReverseAuction.com Inc. Case No 00-0032 (DDC Jan 6, 2000) (consent order)

GeoCities FTC Dkt No C-3849 (Feb 12, 1999) (consent order)

In the Matter of ASUSTeK Computer Inc FTC Dkt No C-4587 (Jul 28, 2016) (consent order)

In the matter of BLU Products and Samuel Ohev-Zion FTC Dkt No C-4657 (Sep 10, 2018) (consent order)

In the Matter of Facebook Inc FTC Dkt No C-4365 (Jul 27, 2012) (original consent order) and (Apr 28, 2020) (modified consent order)

In the Matter of Fandango LLC FTC Dkt No C-4481 (Aug 24, 2014) (consent order)

In the matter of Goldenshores Technologies, LLC and Erik M. Geidl FTC Dkt No C-4446 (Apr 9, 2014) (consent order)

In the matter of Google Inc. FTC Dkt No C-4336 (Oct 13, 2011) (consent order)

In the Matter of HTC America Inc. FTC Dkt No C-4406 (Jul 25, 2013) (consent order)

In the matter of James v Grago, Jr. doing business as ClixSense.com FTC Dkt No C-4678 (Jul 2, 2019) (consent order)

In the Matter of PayPal Inc. FTC Dkt No C-4651 (May 24, 2018) (consent order)

Liberty Financial Companies Inc. FTC Dkt No C-3891 (Aug 12, 1999)

McDonough v. Fallon McElligott Inc 40 U.S.P.Q.2d (BNA) 1826, 1828 (S.D. Cal. 1996)

United States of America and People of the State of New York v Google LLC and YouTube LLC Case No 1:19-cv-02642 (DDC Sep 10, 2019) (draft consent order)

United States of America v Musical.ly Case No 2:19-cv-01439 (CD Cal Feb 27, 2019) (proposed consent order)

United States of America v Unixiz Inc and others Case No 5:19-cv-2222 (ND Cal Apr 24, 2019)

United States v Bigmailbox.Com Inc Case No 01–606–B (ED Va Apr 18, 2001)

United States v Bonzi Software Inc Case No CV–04–1048 (CD Cal Feb 17, 2004)

United States v Dish Network LLC 2010 US Dist LEXIS 8957, 10 (CD Ill Feb 3, 2010)

United States v Facebook Inc Case No 1:19-cv-02184, related FTC Dkt No C-4365 (DDC Jul 24, 2019) (consent order)

United States v Godwin Case No 1:11–cv–03846–JOF (ND Ga Feb 1, 2012)

United States v Industrious Kid Inc Case No CV–08–0639 (ND Cal,filed Jan 28, 2008)

United States v InMobi Pte Ltd Case No 3:16-cv-03474 (ND Cal Jun 22, 2016)

United States v LAI Systems LLC Case No 2:15-cv-09691 (CD Cal Dec 17, 2015)

United States v Looksmart Ltd Case No 01–605–A (ED Va Apr 18, 2001)

United States v Prime Sites Inc. Case No 2:18-cv-00199 (D Nev May 2, 2018)

United States v Retro Dreamer and Craig E. Sharpe and Gavin S. Bowman Case No 5:15-cv-02569 (CD Cal Dec 17, 2015)

United States v RockYou Inc Case No 3:12–cv–01487–SI (ND Cal Mar, 27, 2012)

United States v V Tech Electronics Ltd and VTech Electronics North America LLC Case No 1:18-cv-114 (ND Ill Aug 1, 2018)

United States v Xanga.com Inc Case No 06–CIV–6853 (SDNY Sept 11, 2006)

United States v. W3 Innovations LLC Case No CV–11–03958 (ND Cal Aug 12, 2011)

Zippo Manufacturing Co v Zippo Dot Com Inc 952 F. Supp. 1119 (W.D. Pa. 1997)

EUROPEAN UNION

Court of Justice of the European Union

Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) and Federación de Comercio Electrónico y Marketing Directo (FECEMD) v Administración del Estado and others (intervening) (C-468/10 and C-469/10) ECLI:EU:C:2011:777

Aziz v Caixa d'Estalvis de Catalunya, Tarragona i Manresa (Catalunyacaixa) (C-415/11) ECLI:EU:C:2013:164

Bara, Smaranda and Others v Casa Naţională de Asigurări de Sănătate and Others (C-201/14) ECLI:EU:C:2015:638

Breyer, Patrick v Bundesrepublik Deutschland (C-582/14) ECLI:EU:C:2016:779

Bundesverband der Verbraucherzentralen und Verbraucherverbände - Verbraucherzentrale Bundesverband e.V. v Planet49 GmbH [GC] (C-673/17) ECLI:EU:C:2019:801

College van burgemeester en wethouders van Rotterdam v M. E. E. Rijkeboer (C-553/07) ECLI:EU:C:2009:293

Data Protection Commissioner v Facebook Ireland Ltd, Maximillian Schrems and Others (intervening) “Shrems II” (C-311/18) ECLI:EU:C:2020:559

Digital Rights Ireland (C‑293/12 and C‑594/12) ECLI:EU:C:2014:238

Fashion ID GmbH & Co. KG v Verbraucherzentrale NRW eV (C-40/17) ECLI:EU:C:2019:629

Google France SARL and Google Inc v Louis Vuitton Malletier SA and others [GC] (C-236/08 to C-238/08) ECLI:EU:C:2010:159

Google LLC v Bundesrepublik Deutschland (C-193/18) ECLI:EU:C:2019:498

Google Spain SL and Google Inc (C-131/12) ECLI:EU:C:2014:317

Google LLC, successor in law to Google Inc. v Commission nationale de l'informatique et des libertés (CNIL) “Google (Territorial scope of de-referencing)” [GC] (C-507/17) ECLI:EU:C:2019:772

Huber, Heinz v Bundesrepublik Deutschland (C-524/06) ECLI:EU:C:2008:724

Institut professionnel des agents immobiliers (IPI) v Geoffrey Englebert and Others (C-473/12) ECLI:EU:C:2013:715

Jehovan todistajat [GC] (C-25/17) ECLI:EU:C:2018:551

Lindqvist (C-101/01) ECLI:EU:C:2003:596

L’Oréal SA and Others v eBay International AG and Others [GC] (C-324/09) ECLI:EU:C:2011:474

Pfeiffer, Roith, Süß, Winter, Nestvogel, Zeller, Döbele [GC] (C-397/01 to C-403/01) ECLI:EU:C:2004:584

Puškár, Peter v Finančné riaditeľstvo Slovenskej republiky and Kriminálny úrad finančnej správy (C-73/16) ECLI:EU:C:2017:725

SABAM v Netlog (C-360/10) ECLI:EU:C:2012:85

Scarlet Extended v Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM) (C-70/10) ECLI:EU:C:2011:771

Schrems, Maximillian v Data Protection Commissioner (C-362/14, EU:C:2015:650)

Skype Communications Sàrl v Institut belge des services postaux et des télécommunications (IBPT) (C-142/18) ECLI:EU:C:2019:460

UPC DTH Sàrl v Nemzeti Média- és Hírközlési Hatóság Elnökhelyettese (C-475/12) ECLI:EU:C:2014:285

Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde v Rīgas pašvaldības SIA "Rīgas satiksme" (C-13/16) ECLI:EU:C:2017:336

Wirtschaftsakademie Schleswig-Holstein (C-210/16) ECLI:EU:C:2018:388

European Court of Human Rights

I v Finland no 20511/03, ECHR 2008

Von Hannover v. Germany (no. 2) [GC], nos 40660/08 and 60641/08, ECHR 2012

M.L. and W.W. v Germany no 60798/10 and 65599/10, ECHR, 2018

GERMANY

Vorratsdatenspeicherung [Data retention] 125 BVerfGE 260 (2010) [English translation available at https://wwwbundesverfassungsgerichtde/ entscheidungen/rs20100302_1bvr025608htmll; accessed on 27 July 2019]

BIBLIOGRAPHY

Books

Bainbridge D, *Data Protection Law* (2 edn, XPL 2005)

Bennet CJ, *Regulating privacy : data protection and public policy in Europe and the United States* (Cornell University Press 1992)

Bishop M and Woolman S, 'Freedom and Security of the Person' in Woolman S and Bishop M (eds), *Constitutional Law of South Africa*, vol 3 (2 edn, Juta 2014)

Burns Y and Burger-Smidt A, *A Commentary on the Protection of Personal Information Act* (LexisNexis 2018)

Bygrave LA, *Data Protection Law−Approaching Its Rationale, Logic and Limits* (Kluwer International 2002)

Bygrave LA, *Data Privacy Law: An International Perspective* (Oxford Scholarship Online 2014)

Bygrave LA, 'Hardwiring Privacy' in Brownsword R, Scotford E and Yeung K (eds), *The Oxford Handbook of Law, Regulation, and Technology* (OUP 2017)

Carey P and Treacy B, *Data protection : a practical guide to UK and EU law* (4 edn, OUP 2015)

Cate FH, *Privacy in the Information Age* (Brookings Institution Press 2000)

Cate FH, 'The Failure of Fair Information Practice Principles ' in Winn JK (ed), *Consumer Protection in the Age of the 'information Economy'* (Ashgate 2006)

Cavoukian A, 'Privacy by Design: Origins, Meaning, and Prospects for Assuring Privacy and Trust in the Information Era' in Yee GOM (ed), *Privacy Protection Measures and Technologies in Business Organizations: Aspects and Standards* (Aptus Research Solutions Inc. and Carleton University, Canada 2012)

Checkland P and Holwell S, 'Data, capta, information and knowledge' in Hinton M (ed), *Introducing Information Management* (Routledge 2006)

Chertoff M, *Exploding Data: Reclaiming Our Cyber Security in the Digital Age* (Atlantic Monthly Press 2018)

Christie RH and Bradfield G, *Christie's Law of Contract in South Africa* (LexisNexis 2016)

De Vries K and others, 'The German Constitutional Court Judgment on Data Retention: Proportionality Overrides Unlimited Surveillance (Doesn't It?)' in Gutwirth S and others (eds), *Computers, Privacy and Data Protection: an Element of Choice* (Springer Netherlands 2011)

De Wet J and Van Wyk AL, *De Wet en Van Wyk: Die Suid-afrikaanse Kontraktereg en Handelsreg : Volume 1 : Kontraktereg* (Butterworths 1992)

Donnelly DL, 'Data Privacy in the Cloud: The Position of SMMEs Engaged in Mobile App Development in South Africa' in Singh U and others (eds), *Global Trends in Management, IT and Governance in an e-World (E-MIG 2019 International)* (CSSALL Publishers 2020)

Duncan J, *Stopping the Spies: Constructing and resisting the surveillance state in South Africa* (Wits University Press 2018)

Ebeling MFE, *Healthcare and Big Data: Digital Specters and Phantom Objects* (Palgrave Macmillan 2016)

Finneran Dennedy M, Fox J and Finneran TR, *The Privacy Engineer's Manifesto: Getting from Policy to Code to QA to Value* (Apress Open 2014)

Flaherty DH, *Protecting Privacy in Surveillance Societies: The Federal Republic of Germany, Sweden, France, Canada, and the United States* (The University of North Carolina Press 1989)

Grant H and others (eds), *Encyclopedia of Data Protection and Privacy* (Sweet & Maxwell 1989 (looseleaf updates))

Hutchison D and others, *The Law of Contract in South Africa* (OUP 2018)

Ivanova Y, 'Data Controller, Processor or a Joint Controller: Towards Reaching GDPR Compliance in the Data and Technology Driven World' (Forthcoming) in Tzanou M (ed), *Personal Data Protection and Legal Developments in the European Union* (IGI Global, 2020), < https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3584207> accessed 10 August 2020

Jay R, *Data Protection: Law and Practice* (with 1st supplement, 4 edn, Sweet & Maxwell 2014)

Jay R, *Guide to the General Data Protection Regulation* (Sweet & Maxwell 2017)

Kerr AJ, *The Principles of the Law of Contract* (Butterworths 2002)

Kuner C, *European Data Privacy Law and Online Business* (OUP 2003)

Kuner C, *Transborder Data Flows and Data Privacy Laws* (OUP 2013)

Kuner C and others (eds), *The EU General Data Protection Regulation (GDPR): A Commentary* (OUP 2020)

Madsen W, *Handbook of Personal Data Protection* (Palgrave Macmillan 1992)

McComb D, *Semantics in business systems: The savvy manager's guide* (Morgan Kaufmann 2004)

McQuoid-Mason D, 'Privacy' in Woolman S and Bishop M (eds), *Constitutional Law of South Africa*, vol 3 (2 edn, Juta 2014) Neethling J, Potgieter JM and Visser PJ, *Law of delict* (Butterworths 1994)

Neethling J, *Persoonlikheidsreg* (4 edn, Lexis Nexis 2013)

Pasquale F, *The Black Box Society: The Secret Algorithms That Control Money and Information* (Harvard University Press 2015)

Reed C, 'You talkin' to me?' in Schartum DW, Bygrave LA and Bekken AGB (eds), *Jon Bing: En Hyllest / A Tribute* (Gyldendal Akademisk 2014)

Regan PM, *Legislating Privacy: Technology, Social Values, and Public Policy* (2 edn, University of North Carolina Press 1995)

Roos A, 'Data Protection' in Van der Merwe D (ed) *Information and Communications Technology Law* (2 ed, LexisNexis 2016)

Schwab K, *The Fourth Industrial Revolution* (Portfolio Penguin 2017)

Stucke ME and Grunes AP, *Big Data and Competition Policy* (OUP 2016)

Tamò-Larrieux A, *Designing for Privacy and its Legal Framework –Data Protection by Design and Default for the Internet of Things* (Springer 2018)

Van Huyssteen LF, Reinecke MFB and Lubbe GF, *Contract: General Principles* (Juta 2016)

Verga G and others, 'Yet Another Way to Gather People Co-ordinates and its Countermeasures' in Montella R and others (eds), *Internet and Distributed Computing Systems* vol 11874 (IDCS 2019. Lecture Notes in Computer Science, Springer, Cham 2019)

Wacks R, *Personal Information: Privacy and the Law* (OUP 1994)

Walden I, 'Data Protection' in Reed C and Angel J (eds), *Computer Law* (5 edn, OUP 2003)

Westin AF, *Privacy and Freedom* (Athenum 1967)

Zuboff S, *The Age of Surveillance Capitalism - The Fight for a Human Future at the New Frontier of Power* (Profile Books 2019)

Conference papers and conference proceedings

Bincoletto G, 'A Data Protection by Design Model for Privacy Management in Electronic Health Records' in *Annual Privacy Forum: Privacy Technologies and Policy* (Springer, Rome, Italy 13-14 June 2019) 161-181

Binns R and others, ‘It's Reducing a Human Being to a Percentage': Perceptions of Justice in Algorithmic Decisions’ in *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems* (ACM, Montréal, QC 21-26 April 2018) 1-14

Binns R and others, ‘Third Party Tracking in the Mobile Ecosystem’ in *Proceedings of the 10th ACM Conference on Web Science* (ACM, Amsterdam, Netherlands, 27-30 May 2018) 23 – 31

Botha J, Eloff MM and Swart I, ‘Evaluation of Online Resources on the Implementation of the Protection of Personal Information Act in South Africa’ in Zaayman J and Leenan L (eds), *Proceedings of the 10th International Conference on Cyber Warfare and Security ICCWS-2015* (Academic Conferences, Reading 2015)

Celosia G and Cunche M, ‘Discontinued Privacy: Personal Data Leaks in Apple Bluetooth-Low-Energy Continuity Protocols’ (2020) 1 *Proceedings on Privacy Enhancing Technologies* 26-46

Chen T and others, ‘Information Leakage Through Mobile Analytics Services’ in *HotMobile'14: Proceedings of the 15th Workshop on Mobile Computing Systems and Applications* (ACM, Santa Barbara CA 26-27 February 2014) 1-6

Cortesi A and others, ‘Datacentric Semantics for Verification of Privacy Policy Compliance by Mobile Applications’ in *International Workshop on Verification, Model Checking, and Abstract Interpretation* (Springer 2015) 61-79

Joorabchi ME, Mesbah A and Kruchten P, ‘Real challenges in mobile app development’ in *Proceedings of ACM/IEEE International Symposium on Empirical Software Engineering and Measurement* (ACM/IEEE, Baltimore, Maryland 10-11 October 2013)

Kurtz C and Semmann M, ‘Privacy by Design to Comply with GDPR: A Review on Third-Party Data Processors’ (*24th Americas Conference on Information Systems*, New Orleans, 2018)

Kurtz C and others, ‘The Unlikely Siblings in the GDPR Family: A Techno-Legal Analysis of Major Platforms in the Diffusion of Personal Data in Service Ecosystems’ in *Proceedings of the 52nd Hawaii International Conference on System Sciences* (Scholar Space, Grand Waile, Maui 8-11 January 2019) 5059-5068

Leontiadis I and others, ‘Don't Kill My Ads!: Balancing Privacy in an Ad-Supported Mobile Application Market’ in *Proceedings of the Twelfth Workshop on Mobile Computing Systems & Applications* (ACM February 2012) 1-6

Liu Y and others, ‘Identifying Personal Information in Internet Traffic’ in *Proceedings of ACM Conference on Online Social Networks* (ACM, Palo Alto, US 2-3 November 2015)

Martin J and others, ‘A Study of MAC Address Randomization in Mobile Devices and When It Fails’ in *Proceedings on Privacy Enhancing Technologies* (De Gruyter Open, Minneapolis, US 18-21 July 2017)

Mhaidli AH, Zou Y and Schaub F, ‘"We Can't Live Without Them!" App Developers' Adoption of Ad Networks and Their Considerations of Consumer Risks’ in *15th Symposium on Usable Privacy and Security (SOUPS 2019)* (USENIX, Santa Clara, CA, US 11-13 August 2019) 225-244

Narayanan A and Shmatikov V, ‘Robust De-Anonymization of Large Sparse Datasets’ in *2008 IEEE Symposium on Security and Privacy (SP 2008)* (IEEE, Oakland, CA, US 18-21 May 2008) 111-125

Nath S and others, ‘Smart Ads: Bringing Contextual Ads to Mobile Apps’ in *Proceeding of the 11th Annual International Conference on Mobile Systems, Applications, and Services* (ACM, Taipei, Taiwan 25-28 June 2013) 111-124

Okoyomon E and others, ‘On The Ridiculousness of Notice and Consent: Contradictions in App Privacy Policies’ (*The Workshop on Technology and Consumer Protection* (ConPro ’19), 2019)

Omoronyia I and others, ‘Engineering Adaptive Privacy: On the Role of Privacy Awareness Requirements’ in *Proceedings of the 2013 International Conference on Software Engineering (ICSE)* (IEEE, San Francisco, CA, 18-26 May 2013) 632-641

Pandit HJ and others, ‘Creating a Vocabulary for Data Privacy’ in Panetto H and others (eds), *OTM Consolidated International Conferences: On the Move to Meaningful Internet Systems* (Springer, Rhodes, Greece 21-25 October 2019) 714-730

Reardon J and others, ‘50 Ways to Leak Your Data: An Exploration of Apps' Circumvention of the Android Permissions System’ in *Proceedings of the 28th USENIX Security Symposium* (USENIX, Santa Clara, CA, US14–16 August 2019) 603-620

Sheth S, Kaiser G and Maalej W, ‘Us and Them: A Study of Privacy Requirements Across North America, Asia, and Europe’ in *Proceedings of the 36th International Conference on Software Engineering* (ACM, Hyderabad, India 31 May - 7 June 2014) 859-870

Stevens R and others, ‘Investigating User Privacy in Android Ad Libraries’ in *Workshop on Mobile Security Technologies (MoST)*, vol 10 (Citeseer 2012)

Thomas K and others, ‘Distilling Privacy Requirements For Mobile Applications’ in *Proceedings of the 36th International Conference on Software Engineering* (ACM, Hyderabad, India 31 May - 7 June 2014) 871-882

Tiwari T and others, ‘Location Leakage from Network Access Patterns’ in *2019 IEEE Conference on Communications and Network Security (CNS)* (IEEE, Washington DC 10-12 June 2019)

Ullah I and others, ‘Characterising User Targeting for In-App Mobile Ads’ in *2014 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)* (IEEE, Toronto, ON, 22 April - 2 May 2014)

Van Kleek M and others, ‘Better the Devil You Know: Exposing the Data Sharing Practices of Smartphone Apps’ in *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems* (CHI, Denver, Colarado 6-11 May 2017)

Van Kleek M and others, ‘Better the Devil You Know: Exposing the Data Sharing Practices of Smartphone Apps’ in *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems* (CHI, Denver, Colarado 6-11 May 2017)

Vallina-Rodriguez N and others, ‘Tracking the trackers: Towards understanding the mobile advertising and tracking ecosystem’ (*1st Data and Algorithm Transparency Workshop*, New York, NY, 2016)

Wang H and Guo Y, ‘Understanding Third-Party Libraries in Mobile App Analysis’ in *39th International Conference on Software Engineering Companion (ICSE-C)* (IEEE/ACM, Buenos Aires 20-28 May 2017)

Williams E and Yerby J, ‘Google and Facebook Data Retention and Location Tracking through Forensic Cloud Analysis’ in South Association for Information Systems (SAIS) (ed), *SAIS 2019 Proceedings* (2019)

Zang H and Bolot J, ‘Anonymization of Location Data Does Not Work: A Large-Scale Measurement Study’ in *Proceedings of the 17th Annual International Conference on Mobile Computing and Networking* (ACM, Las Vegas 19-23 September 2011)

Journal articles

Acquisti A, Taylor C and Wagman L, ‘The Economics of Privacy’ (2016) 54 (2) *Journal of Economic Literature* 442-492Ananny M and Crawford K, ‘Seeing Without Knowing: Limitations of the Transparency Ideal and its Application to Algorithmic Accountability’ (2018) 20 (3) *New Media & Society* 973-989

Ausloos J, Mahieu R and Veale M, 'Getting Data Subject Rights Right' (2019) 10 (3) *Journal of Intellectual Property, Information Technology and Electronic Commerce Law* 283-309

Bhana D, 'Contractual Autonomy Unpacked: The Internal and External Dimensions of Contractual Autonomy Operating in the Post-Apartheid Constitutional Context' (2015) 31 (3) *SAJHR* 526-552

Black J, 'Regulatory Conversations' (2002) 29 (1) *Journal of Law and Society* 163-196

Blenner S and others, 'Privacy Policies of Android Diabetes Apps and Sharing of Health Information' (2016) 315 (10) *JAMA* 1051-1052

Bonatti PA and others, 'Machine Understandable Policies and GDPR Compliance Checking' [2020] *arXiv preprint arXiv:200108930*

Brand F, 'The Role of Good Faith, Equity and Fairness in the South African Law of Contract: The Influence of the Common Law and the Constitution' (2009) 126 *SALJ* 71-90

Bruening PJ and Culnan MJ, 'Through a Glass Darkly: From Privacy Notices to Effective Transparency' (2016) 17 (4) *NCJL & Tech* 515-580

Budin-Ljøsne I and others, 'Dynamic Consent: A Potential Solution to some of the Challenges of Modern Biomedical Research' (2017) 18 (1) *BMC Medical Ethics* 1-10

Bygrave LA, 'Data Protection by Design and by Default: Deciphering the EU's Legislative Requirements' (2017) 4 (02) *Oslo Law Review* 105-120

Chen MK and Rohla R, 'The Effect of Partisanship and Political Advertising on Close Family Ties' [2017] *arXiv preprint arXiv:171110602*

Daley J, 'Insecure Software is Eating the World: Promoting Cybersecurity in an Age of Ubiquitous Software-embedded Systems' (2017) 19 (3) *Stan Tech L Rev* 533-546

De Hert P and Papakonstantinou V, 'The new General Data Protection Regulation: Still a sound system for the protection of individuals?' (2016) 32 *Computer Law & Security Review* 179-194De Montjoye Y-A and others, 'Unique in the Crowd: The Privacy Bounds of Human Mobility' (2013) 3 *Scientific Reports* 1376

Dehling T and others, 'Exploring the Far Side of Mobile Health: Information Security and Privacy of Mobile Health Apps on iOS and Android' (2015) 3 (1) *JMIR Mhealth Uhealth* e8

Diver L and Schafer B 'Opening the Black Box: Petri Nets and Privacy by Design' (2017) 31 (1) *International Review of Law, Computers & Technology* 68-90

Donnelly D-L, ‘Do You Always Get Something Out? The Impact of the Insurance Act 18 of 2017 and Revised Policyholder Protection Rules on Material Misrepresentation and Non-disclosure’ (2018) 135 (4) *SALJ* 593-612

Esayas S, ‘The Role of Anonymisation and Pseudonymisation under the EU Data Privacy Rules: Beyond the ‘All or Nothing’ Approach’ (2015) 6 (2) *European Journal of Law and Technology* 1-28

Flaherty DH, ‘On the Utility of Constitutional Rights to Privacy and Data Protection’ (1990) 41 *Case W Res L Rev* 831-856

Flavián C and Guinalíu M, ‘Consumer Trust, Perceived Security and Privacy Policy’ (2006) 106 (5) *Industrial Management & Data Systems* 601-620

Flew T, ‘The Platformized Internet: Issues for Internet Law and Policy’ (2019) 22 (11) *Journal of Internet Law* 3-16

Gandomi A and Haider M, ‘Beyond the Hype: Big Data Concepts, Methods, and Analytics.’ (2015) 35 (2) *International Journal of Information Management* 137-144

Gellert R, ‘We Have Always Managed Risks in Data Protection Law: Understanding the Similarities and Differences between the Rights-based and the Risk-based Approaches to Data Protection’ (2016) 2 (4) *European Data Protection Law Review* 481-492

Globocnik J, ‘On Joint Controllership for Social Plugins and Other Third-Party Content–a Case Note on the CJEU Decision in Fashion ID’ (2019) 50 (8) *IIC-International Review of Intellectual Property and Competition Law* 1033-1044

Gorwa R, ‘What is Platform Governance?’ (2019) 22 (6) *Information, Communication & Society* 854-871

Greene D and Shilton K, ‘Platform Privacies: Governance, Collaboration, and the Different Meanings of "Privacy" in iOS and Android Development’ (2018) 20 (4) *New Media and Society* 1640 -1657

Greene D and Shilton K, ‘Platform Privacies: Governance, Collaboration, and the Different Meanings of "Privacy" in iOS and Android Development’ (2018) 20 (4) *New Media & Society* 1640-1657

Grindrod K and others, ‘Locking it Down: The Privacy and Security of Mobile Medication Apps’ (2017) 150 (1) *Can Pharm J (Ott)* 60-66

Grundy Q and others, ‘Data Sharing Practices of Medicines Related Apps and the Mobile Ecosystem: Traffic, Content, and Network Analysis’ (2019) 364 *BMJ* 1920

Hadar I and others, ‘Privacy by Designers: Software Developers’ Privacy Mindset’ (2018) 23 (1) *Empirical Software Engineering* 259-289

Hahn RW and Layne-Farrar A, ‘The Law and Economics of Software Security’ (2006) 30 *Harv JL & Pub Pol'y* 283-354

Hashem IAT and others, ‘The Rise of “Big Data” on Cloud Computing: Review and Open Research Issues’ (2015) 47 *Information Systems* 98-115

Huang J and others, ‘SieveDroid: Intercepting Undesirable Private-Data Transmissions in Android Applications’ (2019) 14 (1) *IEEE Systems Journal* 375-386

Huckvale K and others, ‘Unaddressed Privacy Risks in Accredited Health and Wellness Apps: A Cross-Sectional Systematic Assessment’ (2015) 13 *BMC Medicine* 214-227

Hustinx P, ‘Privacy by Design: Delivering the Promises’ (2010) 3 (2) *Identity in the Information Society* 253-255

Jasmontaite L and others, ‘Data Protection By Design and by Default: Framing Guiding Principles Into Legal Obligations in the GDPR’ (2018) 4 *Eur Data Prot L Rev* 168-189

Katyal SK and Grinvald LC, ‘Platform Law and the Brand Enterprise’ (2017) 32 *Berkeley Tech LJ* 1135-1182

Kerr OS, ‘Applying the Fourth Amendment to the Internet: A General Approach’ (2010) 62 *Stan L Rev* 1005-1049

Ketelaar PE and others, ‘“Opening” Location-Based Mobile Ads: How Openness and Location Congruency of Location-Based Ads Weaken Negative Effects of Intrusiveness on Brand Choice’ (2018) 91 *Journal of Business Research* 277-285

Koops B and Leenes R ‘Privacy Regulation Cannot Be Hardcoded: A Critical Comment on the ‘Privacy by Design’ Provision in Data Protection Law’ (2014) 28 (2) *International Review of Law, Computers & Technology* 159-171

Lambrecht I, Verdoodt V and Bellon J, ‘Platforms and Commercial Communications Aimed at Children: A Playground under Legislative Reform?’ (2018) 32 (1) *International Review of Law, Computers & Technology* 58-79

Lawler JP, ‘Customer Loyalty and Privacy on the Web’ (2003) 2 (1) *Journal of Internet Commerce* 89-105

Liu X and others, ‘Privacy Risk Analysis and Mitigation of Analytics Libraries in the Android Ecosystem’ (2019) 19 (5) *IEEE Transactions on Mobile Computing* 1184-1199

Louw AM, ‘Yet Another Call for a Greater Role for Good Faith in the South African Law of Contract: Can We Banish the Law of the Jungle, While Avoiding the Elephant in the Room?’ (2013) 16 (5) *Potchefstroom Electronic Law Journal* 43-120

Lynksy O, ‘Deconstructing data protection: the “added-value” of a right to data protection in the EU legal order’ (2014) 63(3) *International and Comparative Law Quarterly* 569-597.

Madden M and others, ‘Privacy, Poverty, and Big Data: A Matrix of Vulnerabilities for Poor Americans’ (2017) 95 *Wash UL Rev* 53-125

Mahieu R, van Hoboken J and Asghari H, ‘Responsibility for Data Protection in a Networked World: On the Question of the Controller, Effective and Complete Protection and Its Application to Data Access Rights in Europe’ (2019) 10 (1) *Journal of Intellectual Property, Information Technology and Electronic Commerce Law* 84-104

Martin K and Shilton K, ‘Putting Mobile Application Privacy in Context: An Empirical Study of User Privacy Expectations For Mobile Devices’ (2016) 32 (3) *The Information Society* 200-216

Mashinini N, ‘The processing of personal information using remotely piloted aircraft systems in South Africa’ (2020) 53 (1) *De Jure* 140 – 158

Millard C, ‘At this rate, everyone will be a [joint] controller of personal data!' (2019) 9 (4) *International Data Privacy Law* 217-219

Neethling J, ‘The Concept of Privacy in South African Law’ (2005) 122 (1) *SALJ* 18-22

Njotini MN, ‘Preserving the Integrity of Medical-related Information – How "Informed" is Consent?’ (2018) 21 (1) *Potchefstroom Electronic Law Journal* 1-20

Okediran O and others, ‘Mobile Operating Systems and Application Development Platforms: A Survey’ (2014) 6 (1) *International Journal of Advanced Networking and Applications* 2195-2201

Papageorgiou A and others, ‘Security and Privacy Analysis of Mobile Health Applications: The Alarming State of Practice’ (2018) 6 *IEEE Access* 9390-9403

Paranjothi A, Khan MS and Nijim M, ‘Survey on Three Components of Mobile Cloud Computing: Offloading, Distribution and Privacy’ (2017) 5 (6) *Journal of Computer and Communications* 1-31

Pistorius T, ‘Click-wrap and Web-wrap Agreements’ (2004) 16 *S Afr Mercantile LJ* 568-576

Ratz M, ‘Damages Arising from Contraventions of Competition Act 89 of 1998’ (2019) 22 *PER* 26.

Ramadan Q and others, ‘A Semi-automated BPMN-based Framework for Detecting Conflicts between Security, Data-minimization and Fairness Requirements’ [2020] *Software and Systems Modeling* 1-37

Reidenberg JR, ‘Resolving Conflicting International Data Privacy Rules in Cyberspace’ (2000) 52 (5) *Stan L Rev* 1315–1371

Rocher L, Hendrickx JM and de Montjoye Y, ‘Estimating the Success of Re-identifications in Incomplete Datasets Using Generative Models’ (2019) *Nature Communications* 10:3069

Roos A, ‘Privacy in the Facebook Era: A South African Legal Perspective’ (2012) 129 (2) *SALJ* 375-402

Roos A, ‘Data Protection: Explaining the International Backdrop and Evaluating the Current South African Position’ (2007) 124 *SALJ* 400-437

Rubinstein IS, ‘Regulating Privacy by Design’ (2011) 26 *Berkeley Tech LJ* 1409-1546

Rubinstein IS and Good N, ‘Privacy by Design: A Counterfactual Analysis of Google and Facebook Privacy Incidents’ (2013) 28 *Berkeley Tech LJ* 1333-1414

Schwartz PM, ‘Beyond Lessig's Code for Internet Privacy: Cyberspace Filters, Privacy Control, and Fair Information Practices’ [2000] *Wis L Rev* 743-788

Schwartz PM, ‘Preemption and Privacy’ (2008) 118 *Yale LJ* 902-947

Schwartz PM, ‘The EU-US Privacy Collision: A Turn to Institutions and Procedures’ (2012) 126 *Harv L Rev* 1966-2009

Schwartz PM and Solove DJ, ‘The PII Problem: Privacy and a New Concept of Personally Identifiable Information’ (2011) 86 *NYUL Rev* 1814-1894

Senarath A and Arachchilage NAG, ‘Understanding Software Developers' Approach Towards Implementing Data Minimization’ *arXiv preprint arXiv:180801479*

Senarath A and Arachchilage NAG, ‘A Data Minimization Model For Embedding Privacy Into Software Systems’ (2019) 87 (101605) *Computers & Security* 1-17

Shilton K and Greene D, ‘Linking Platforms, Practices, and Developer Ethics: Levers for Privacy Discourse in Mobile Application Development’ (2019) 155 (1) *Journal of Business Ethics* 131-146

Staunton C and others, ‘Safeguarding the Future of Genomic Research in South Africa: Broad Consent and the Protection of Personal Information Act No. 4 of 2013’ (2019) 109 (7) *South African Medical Journal* 468-470

Sunyaev A and others, ‘Availability and Quality of Mobile Health App Privacy Policies’ (2015) 22 *Journal of the American Medical Informatics Association* 1-4

Susser D, ‘Notice After Notice-and-Consent: Why Privacy Disclosures Are Valuable Even If Consent Frameworks Aren't’ (2019) 9 *Journal of Information Policy* 37-62

Sweeney L, ‘K-anonymity: A Model for Protecting Privacy’ (2002) 10 (5) *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems* 557-570

Tene O, ‘Privacy Law's Midlife Crisis: Critical Assessment of the Second Wave of Global Privacy Laws.’ (2013) 74 (6) *Ohio State Law Journal* 1217-1262

Townsend BA and Thaldar DW, ‘Navigating Uncharted Waters: Biobanks and Informational Privacy in South Africa’ (2019) 35 (4) *South African Journal on Human Rights* 329-350

Van Alsenoy B, ‘Liability under EU Data Protection Law: From Directive 95/46 to the General Data Protection Regulation’ (2016) 7 (3) *Journal of Intellectual Property, Information Technology & Electronic Commerce Law* 271-288

Van Rest J and others, ‘Designing Privacy-by-Design’ [2014] *Privacy Technologies and Policy* 55

Veale M and Binns R, ‘Fairer Machine Learning in the Real World: Mitigating Discrimination Without Collecting Sensitive Data’ (2017) 4 (2) *Big Data & Society* 1-17

Wachter S, Mittelstadt B and Floridi L, ‘Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation’ (2017) 7 (2) *International Data Privacy Law* 76-99

Waldman AE, ‘Privacy's Law of Design’ (2018) 9 *UC Irvine L Rev* 1239

Zarour K and others, ‘A Systematic Literature Review on BPMN Extensions’ [2019] *Business Process Management Journal*, https://doi.org/10.1108/BPMJ-01-2019-0040.

Newspaper articles

Editorial, ‘Zoom Slapped with Class Action Lawsuit over Facebook Data-sharing Issues’ *Engineering & Technology* (1 April 2020) <https://eandt.theiet.org/content/articles/2020/04/zoom-slapped-with-class-action-lawsuit-over-facebook-data-sharing-issues/> accessed 4 April 2020

Hakim D and Singer N, ‘New York Attorney General Looks Into Zoom’s Privacy Practices’ *New York Times* (30 March 2020) <https://www.nytimes.com/2020/03/30/technology/new-york-attorney-general-zoom-privacy.html> accessed 4 April 2020

Hern A, ‘Cambridge Analytica: How Did It Turn Clicks into Votes?’ *The Guardian* (6 May 2018) <https://www.theguardian.com/news/2018/may/06/cambridge-analytica-how-turn-clicks-into-votes-christopher-wylie> accessed 26 February 2020

Isaac M and Frenkel S, 'Facebook Security Breach Exposes Accounts of 50 Million Users' *NY Times* (28 September 2018) <https://www.nytimes.com/2018/09/28/technology/facebook-hack-data-breach.html> accessed 8 March 2020

Nieselow T, 'Five Massive Data Breaches Affecting South Africans' *Mail & Guardian* (19 June 2018) <https://mg.co.za/article/2018-06-19-five-massive-data-breaches-affecting-south-africans/> accessed 8 March 2020

Command papers, guidelines, reports and industry standards

Asia-Pacific Economic Cooperation

APEC, *APEC Privacy Framework* (APEC#205-SO-012, 2005)

APEC, *APEC Privacy Framework (2015)* (APEC#217-CT-019, 2017)

Council of Europe

Council of Europe, Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108), *Guidelines on the Protection of Individuals with regard to the Processing of Personal Data in a World of Big Data* (Strasbourg, 23 January 2017)(T-PD(2017)01)

Council of Europe, Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108) *Artificial Intelligence and Data Protection: Challenges and Possible Remedies* (Strasbourg, 25 January 2019(T-PD(2018)09Rev)

Council of Europe, *Explanatory Report to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data* (Strasbourg, 28 January 1981)

Council of Europe, *128th Session of the Committee of Ministers (Elsinore, Denmark, 17-18 May 2018) - Ad hoc Committee on Data Protection (CAHDATA) – Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108) - Explanatory report.* (CM(2018)2-addfinal, 2018)

Council of Europe (Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data), *Guidelines on ihe Protection of Individuals with regard to the Processing of Personal Data in a World of Big Data* (T-Pd(2017)01, 23 January 2017)

Council of the European Union

Council of European Union, *Presidential proposal 14054/19* (2017/0003(COD), 15 November 2019)

Council of European Union, *Presidential proposal 5979/20* (2017/0003(COD), 21 February 2020)

East African Community

East African Community (EAC), *Draft EAC Framework for Cyberlaws* (November 2008)

European Commission

European Commission, Recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises (C(2003) 1422, OJ L 124/36, 25 May 2003)

European Commission, Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the regions: "A Comprehensive Approach on Data Protection in the European Union" (COM(2010) 609 final, 2010)

European Commission, Commission Staff Working Paper Impact Assessment (SEC(2012) 72 final, 2012)

European Commission, Safeguarding Privacy in a Connected World. A European Data Protection Framework for the 21st century (COM(2012) 9 final, 2012)

European Commission, e-Government Core Vocabularies Handbook (2016)

European Commission (Expert group on cloud computing contracts), Discussion Paper: Meeting of 19 & 20 November 2013 (2013)

European Network and Information Security Agency (Now European Union Association for Cybersecurity)

European Network and Security Agency, Privacy and Data Protection by Design: From Policy to Engineering (2014)

European Network and Security Agency, Guidelines for SMEs on the Security of Personal Data Processing (2016)

European Network and Security Agency, Technical Guideline on Security measures for Article 4 and Article 13a Version 1.0 (December 2014)

European Union Agency For Network and Information Security, Privacy by Design in Big Data: An Overview of Privacy by Design in the Era of Big Data Analytics (December 2015)

European Union Agency For Network and Information Security, Privacy and Data Protection in Mobile Applications: A Study on the App Development Ecosystem and the Technical Implementation of GDPR (November 2017)

Industry associations, professional bodies and privacy watchdogs

American Institute of Certified Public Accountants (AICPA) and Canadian Institute of Chartered Accountants (CICA) Privacy Task Force, *Privacy Maturity Model* (March 2011)

Annalect Group, *Internet Users' Response to Consumer Online Privacy* (2012)

App Developers Alliance, *Developers See the Need for Best Practices in Data Sharing & Security, Spring 2018 Data Survey of 100+ Developers and Appreneurs* (2018)

CTIA The Wireless Association, *Best Practices and Guidelines for Location Based Services v2* (2010)

Digital Advertising Alliance, *Self-Regulatory Principles for Online Behavioural Advertising* (2009)

Digital Advertising Alliance, *Self-Regulatory Principles for Multi-Site Data* (2011)

Digital Advertising Alliance, *Application of Self-Regulatory Principles to the Mobile Environment* (2013)

Digital Advertising Alliance, *DAA Ad Marker Implementation Guidelines for Mobile* (2014)

Digital Advertising Alliance, *Application of the DAA Principles of Transparency and Control to Data Used Across Devices* (2017)

Digital Advertising Alliance, *Application of the Self-Regulatory Principles of Transparency & Accountability to Political Advertising* (2018)

Electronic Frontier Foundation, *Mobile User Privacy Bill of Rights* (2012)

Electronic Privacy Information Centre, *Privacy Guidelines for the National Information Infrastructure: A Review of the Proposed Principles of the Privacy Working Group* (Report 94-1, 1995)

EU CLOUD COC, *EU Data Protection Code of Conduct for Cloud Service Providers* (2018)

Future of Privacy Forum, *Cross Device: Understanding the State of State Management* (November 2015)

Future of *Privacy* Forum and Center for Democracy and Technology, *Best Practices for Mobile Applications Developers* (December 2011)

GSM Association, *Privacy Design Guidelines for Mobile Application Development* (February 2012)

GSM Association, *Mobile Privacy Principles: Promoting Consumer Privacy in the Mobile Ecosystem* (January 2011)

Interactive Advertising Bureau, *IAB Mobile Location Data Guide for Publishers* (New York, 2016)

Interactive Advertising Bureau, *IAB CCPA Compliance Framework for Publishers & Technology Companies (Draft for Public Comment)* (October 2019)

Network Advertising Initiative, *2015 Update to the NAI Mobile Application Code* (2015)

Network *Advertising* Initiative, *Guidance for NAI Members: Opt-In Consent* (November 2019)

TrustArc, *Truste's Privacy-by-Design Guidelines* (2012)

Industry standards and technical specifications

Bruton P and others, *Classification of Everyday Living Version 1.0.* (OASIS Committee Specification 02, 26 June 2018)

Cavoukian A and others, *Privacy by Design Documentation for Software Engineers Version 1.0.* (OASIS Committee Specification Draft 01, 25 June 2014)

Garijo D and Gil Y, *The P-PLAN Ontology* (12 March 2014)

Iannella R and McKinney JM, *vCard Ontology - for describing People and Organizations* (W3C Interest Group Note, 22 May 2014) IEEE, *P7012 - Standard for Machine Readable Personal Privacy Terms* (2017)

Institute of Electrical and Electronics Engineers Standards Board, *IEEE Standard Glossary of Software Engineering Terminology* (IEEE, New York, 1990)

ISO, *Information technology — Online privacy notices and consent* (ISO/IEC FDIS 29184 [ISO/IEC DIS 29184])

ISO, *Information technology — Online privacy notices and consent* (ISO/IEC FDIS 29184)

ISO, *Software engineering — Lifecycle profiles for Very Small Entities (VSEs)* (ISO/IEC 29110-2-1:2015)

ISO, *Information technology — Security techniques — Privacy framework* (ISO/IEC 29100, 2011)

ISO, *Common Criteria for Information Technology Security Evaluation v3.1 rev 5* (CC v31 Release 5 ISO/IEC 15408, 2017)

ISO, *Information technology — Security techniques — Guidelines for privacy impact assessment* (ISO/IEC DIS 29134, 2017)

ISO, *Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines* (ISO/IEC 27701, 2019)

Lizar M and Turner D, *Consent Receipt Specification v1.1.0.* (Kantara Initiative Recommendation, 20 February 2018)

Maler E and ForgeRock, *User-Managed Access (UMA) 2.0 Grant for OAuth 2.0 Authorization* (Kantara Initiative Recommendation, 1 July 2018)

National Institute of Standards and Technology (NIST), *Digital Identity Guidelines SP 800-63-3* (2017)

National Institute of Standards and Technology (NIST) and Commerce UDo, *Security Requirements for Cryptographic Modules* (FIPS 140-2, 25 May 2001)

National Institute of Standards and Technology (NIST) and Commerce UDo, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)* (NIST Special Publications 800-122, April 2010)

National Institute of Standards and Technology (NIST) and US Department of Commerce, *Security and Privacy Controls for Federal Information Systems and Organizations* (NIST Special Publication rev 4, 1 April 2015)

National Institute of Standards and Technology (NIST) and *others*, *Federal Enterprise Architecture Security and Privacy Profile (FEA-SPP) v 3.0* (September 2010)

OASIS, *Privacy Management Reference Model and Methodology (PMRM) Version 1.0.* (2013)Object Management Group (OMG), *Business Process Model and Notation (BPMN) v2.02* (ISO/IEC 19510, January 2014)

Pandit HJ and Polleres A, *Data Privacy Vocabulary v0.1 Draft Community Group Report* (Data Privacy Vocabularies *and* Controls Community Group, W3C Consortium, 28 November 2019)

Payment Card Industy Security *Standards* Council, *PCI Data Security Standard v3.2* (2016)

Snell *JM* and Prodromou E, *Activity Streams 2.0* (W3C Recommendation, 23 May 2017)

Tim L, *Sahoo* S and McGuinness D, *PROV-O: The PROV ontology : W3C recommendation 30 April 2013* (W3C Recommendation, 2013)

Villata S and Iannella R, *ODRL Information Model 2.2* (W3C Recommendation, 15 February 2018)

World Wide Web *Consortium* (W3C), *Web Application Privacy Best Practices W3C Working Group Note* (3 July 2012)

International Telecommunications Union

Data Protection: Southern African Development Community (SADC) Model Law (Geneva, 2013)

Measuring the Information Society Report Executive Summary 2018 (2018)

Standardisation Sector (ITU-T), Technical Framework for Countering Mobile In-Application Advertising Spam (Recommendation ITU-T X1249, 2019)

Standardisation Sector (ITU-T), X.509: Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks (October 2016)

International Working Group On Data Protection In Telecommunications

Working Paper on Big Data and Privacy: Privacy principles under pressure in the age of Big Data analytics (May 2014, Skopje, 2014)

Organisation for Economic Co-Operation and Development (OECD)

Organisation for Economic Co-Operation and Development, *An Introduction to Online Platforms and Their Role in the Digital Transformation* (OECD) (2019)

Organisation for Economic Co-Operation and Development, *Cancún Ministerial Declaration on the Digital Economy* (OECD) (2016)

Organisation for Economic Co-Operation and Development, *Explanatory Memorandum to the OECD Privacy Guidelines (*OECD) (*1980)*

Organisation for Economic Co-Operation and Development, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (*OECD) (*1980)*

Organisation for Economic Co-Operation and Development, *The OECD Privacy Framework (*OECD) (*2013)*

Organisation for Economic Co-Operation and Development, *Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data* (OECD) (C(80)58/FINAL, as amended on 11 July 2013 by C(2013)79, 2013)

Organisation for Economic Co-Operation and Development, *Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy (*OECD) (*2007)*

*Thirty Years After the OECD Privacy Guidelines (*OECD) (*2011)*

Organisation for Economic Co-operation and Development (Committee on Digital Economy Policy), Resolution of the Council ([C(2018)141, and C/M(2018)xx, item xxx]) *Draft Resolution of the Council Renewing and Revising the Mandate of the Committee on Digital Economy Policy* (OECD) (2018)

Weber V and Carblanc A, Cloud computing: The concept, impacts and the role of government policy (OECD, Paris) (2014)

South African Government Departments

Department of Telecommunications and Postal Services, *National Integrated ICT Policy White Paper* (GN 1212 in *GG* 40325 of 3 October 2016)

Department of Telecommunications and Postal Services, *The Amended Information and Communication Technology (ICT) Broad-Based Black Economic (B-BBEE) Sector Code* (GN 1381 in *GG* 40407 of 7 November 2016)

Department of Telecommunications and Postal Services, *Electronic Communications Act (36/2005): Final Information and Communication Technology Small, Medium and Micro-Enterprise Development Strategy (Final ICT SMME Development Strategy)* (GN 1252 in *GG* 41243 of 10 November 2017)

Department of Telecommunications and Postal Services, *Electronic Communications and Transactions Act (25/2002): National e-Government Strategy and Roadmap* (GN 341 in *GG* 40772 of 7 April 2017)

Department of Telecommunications and Postal Services, *Electronic Communications and Transactions Act (25/2002): National e-Strategy Digital Society South Africa* (GN 887 in *GG* 41242 of 10 November 2017)

Department of the Presidency, Republic of South Africa (National Planning Commission), *National Development Plan 2030: Our Future – Make it Work* (2011)

Department of the Presidency, Republic of South Africa (National Planning Commission), *National Development Plan Vision for 2030* (2011)

South African Law Reform Commission

South African Law Reform Commission, Discussion Paper 109 Project 124 ‘Privacy and data protection’ (October 2005)

South African Law Reform Commission, Issue Paper 24 Project 124 'Privacy and data protection' (2003)

South African Law Reform Commission, Project 124 'Privacy and data protection' (2009)

State of California: Office of the Attorney General

State of California: Office of the Attorney General, Agreement to Strengthen Privacy Protections for Users of Mobile Applications (22 February 2012)

State of California: Office of the Attorney General, Mobile Applications and Mobile Privacy Fact Sheet (2012)

State of California: Office of the Attorney General, Privacy on the Go: Recommendations for the Mobile Ecosystem (2013)

United Nations

UNCTAD, Data protection regulations and international data flows: Implications for trade and development (2016)

United Nations Development Group (UNDG), Data Privacy, Ethics and Protection: Guidance Note on Big Data for Achievement of the 2030 Agenda (2017)

United States Federal Government Departments

Department of Homeland Security (DHS) Privacy Office, *Handbook for Safeguarding Sensitive PII, Privacy Policy Directive 047-01-007, Revision 3* (2017)

National Telecommunications and Information Administration (NTIA) United States Department of Commerce, *Short Form Notice Code of Conduct to Promote Transparency in Mobile App Practices* (2013 July 25)

US Department of Commerce (Internet Policy Task Force), *Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework* (16 December 2010)

US Department of Health Education and Welfare, *Records, Computers and the Rights of Citizens* (1973)

US Govt. Information Infrastructure Task Force (IITF) Privacy Working Group, *Privacy and the National Information Infrastructure: Principles for Providing and Using Personal Information* (6 June 1995)

US White House Office, *The Framework for Global Electronic Commerce* (1997)

US White House Office, *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy* (February 2012)

United States Federal Trade Commission

Federal Trade Commission, Beyond Voice: Mapping the Mobile Marketplace (April 2009)

Federal Trade Commission, Children's Online Privacy Protection Rule: A Six-Step Compliance Plan for Your Business (June 2017)

Federal Trade Commission, Data Breach Response: A Guide for Business (May 2019)

Federal Trade Commission, Mobile Apps for Kids: Current Privacy Disclosures are Disappointing (February 2012)

Federal Trade Commission, Mobile Apps for Kids: Disclosures Still Not Making the Grade (December 2012)

Federal Trade Commission, Mobile Privacy Disclosures Building Trust Through Transparency (February 2013)

Federal Trade Commission, Mobile Security Updates: Understanding the Issues (February 2018)

Federal Trade Commission, Paper, Plastic ... or Mobile? An FTC Workshop on Mobile Payments (March 2013)

Federal Trade Commission, Privacy Online: A Report to Congress (1998)

Federal Trade Commission, Privacy Online: Fair Information Practices in the Electronic Marketplace: A Report to Congress (May 2000)

Federal Trade Commission, Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers (March 2012)

Federal Trade Commission, Self-regulation and Privacy Online: A Report to Congress (July 1999)

Federal Trade Commission, Start with Security: A Guide for Business (June 2015)

Federal Trade Commission, What's the Deal? An FTC Study on Mobile Shopping Apps (August 2014)

Rosch, J. Thomas: Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers (26 March 2012)

Rosch J. Thomas, *Dissenting Statement of Commissioner: In the Matter of M. Catherine Higgins*, File No. 051 0252

Other

Internet Society (ISOC) and Commission of the African Union, *Personal Data Protection Guidelines for Africa* (2018)

IST-Africa, *Report on ICT Initiatives, Research and Innovation Priorities and Capacity in IST-Africa Partner Countries* (IST Africa-Consortium, October 2017)

Mulligan M and Card D, *Sizing the EU App Economy* (Gigaom Research and European Commission Eurapp Project, February 2014)

Pew Research Center, *Smartphone Ownership is Growing Rapidly Around the World, but Not Always Equally* (February 2019)

Privacy International, *How Apps on Android Share Data with Facebook (even if you don't have a Facebook account)* (2018)

Privacy Protection Study Commission, *Personal Privacy in an Information Society* (US Govt Printing Office, Washington, 1977)

Schofield A, *Research Study on the Economic Impact of Cloud Services on South African SMMEs* (Johannesburg, Johannesburg Centre for Software Engineering: University of Witwatersrand, 2013)

Statistics South Africa, *Standard Industrial Classification of All Economic Activities (SIC)* (7 edn, Stats SA 2012)

Data Protection Authority Publications

Conference of Data Protection and Privacy Commissioners

International Conference of Data Protection and Privacy Commissioners (32nd session), *Resolution on Privacy by Design* (Jerusalem, 29 October 2010)

International Data Protection Commissioners Conference (28th session), *Global Privacy Standard Resolution* (London, 3 November 2006)

Spanish Data Protection Authority, 'Joint Proposal for a Draft of International Standards on the Protection of Privacy with regard to the processing of Personal Data (The Madrid Resolution)' (International Conference of Data Protection and Privacy Commissioners, Madrid, 5 November 2009)

Canada

Information And Privacy Commissioner, Ontario

Cavoukian A, Privacy by Design The 7 Foundational Principles Implementation and Mapping of Fair Information Practices (Information and Privacy Commissioner, Ontario, Canada, 2010)

Cavoukian A, Privacy by Design in Law, Policy and Practice A White Paper for Regulators, Decision-makers and Policy-makers (Information and Privacy Commissioner, Ontario, Canada, 2011)

Cavoukian A, Privacy by Design Strong Privacy Protection – Now, and Well into the Future a Report on the State of PbD to 33rd International Conference of Data Protection and Privacy Commissioners (Toronto, ON, Canada: Office of the Privacy Commissioner, Ontario, Canada, 2011)

Cavoukian A, Privacy by Design and the Emerging Personal Data Ecosystem (Toronto, ON, Canada: Office of the Privacy Commissioner, Ontario, Canada, 2012)

Cavoukian A and Popa C, Privacy by ReDesign: A Practical Framework for Implementation (Toronto, ON, Canada: Office of the Privacy Commissioner, Ontario, Canada, 2011)

Cavoukian A and Prosch M, The Roadmap for Privacy by Design in Mobile Communications: A Practical Tool For Developers, Service Providers, and Users (Toronto, ON, Canada: Office of the Privacy Commissioner, Ontario, Canada, 2010)

Cavoukian A, Shapiro S and Cronk RJ, Privacy Engineering: Proactively Embedding Privacy, by Design (IPC, Ontario Canada, 2014)

Cavoukian A, Privacy by Design The 7 Foundational Principles (Information and Privacy Commissioner, Ontario, Canada, 2009, revised January 2011)

Information and Privacy Commissioner Ontario Canada, The Roadmap for Privacy by Design in Mobile Communications: A Practical Tool for Developers, Service Providers, and Users (2010)

Information and Privacy Commissioner Ontario Canada, Privacy by Design and the Emerging Personal Data Ecosystem (2012)

Information and Privacy Commissioner Ontario Canada and Registratiekamer The Netherlands, Privacy-Enhancing Technologies: The Path to Anonymity (volume 1) (1995)

Office of the Privacy Commissioner of Canada

Office of the Privacy Commissioner of Canada, *Processing Personal Data Across Borders Guidelines* (2009)

Office of the Privacy Commissioner of Canada, *Reaching for the Cloud(s): Privacy Issues related to Cloud Computing* (2010)

Office of the Privacy Commissioner of Canada, *Report on the 2010 Office of the Privacy Commissioner of Canada's Consultations on Online Tracking, Profiling and Targeting, and Cloud Computing* (2011)

Office of the Privacy Commissioner of Canada, *Cloud Computing For Small- And Medium-Sized Enterprises: Privacy Responsibilities and Considerations* (2012)

Office of the Privacy Commissioner of Canada, *Seizing Opportunity: Good Privacy Practices for Developing Mobile Apps* (2012)

Office of the Privacy Commissioner of Canada, Office of the Information and Privacy Commissioner of Alberta and Office of the Information and Privacy Commissioner for British Columbia, *Getting Accountability Right with a Privacy Management Program* (2012)

Office of the Privacy Commissioner of Canada, Office of the Information and Privacy Commissioner of Alberta and Office of the Information and Privacy Commissioner for British Columbia, *Securing Personal Information: A Self-Assessment Tool for Organizations* (2012)

Europe

Article 29 Data Protection Working Party

Article 29 Data Protection Working Party, *Opinion 8/2001 on the Processing of Personal Data in the Employment Context* (WP 48, 13 September 2001)

Article 29 Data Protection Working Party, *Opinion 5/2004 on Unsolicited Communications for Marketing Purposes under Article 13 of Directive 2002/58/EC* (WP 90, 27 February 2004)

Article 29 Data Protection Working Party, *Working Party 29 Opinion on the Use of Location Data with a View to Providing Value Added Services* (WP 115, 25 November 2005)

Article 29 Data Protection Working Party, *Opinion 10/2006 on the Processing of Personal Data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT)* (WP 128, 23 November 2006)

Article 29 Data Protection Working Party, *Working Document on the Processing of Personal Data relating to Health in Electronic Health Records (EHR)* (WP 131, 15 February 2007)

Article 29 Data Protection Working Party, *Opinion 4/2007 on the concept of personal data* (WP 136, 20 June 2007)Article 29 Data Protection Working Party, *Opinion 5/2009 on Online Social Networking* (WP 163, 12 June 2009)

Article 29 Data Protection Working Party and Working Party on Police and Justice, 'The Future of Privacy: Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data' (WP 168, 01 December 2009) *European Commission, Directorate General Justice, Freedom and Security*Article 29 Data Protection Working Party, *Opinion 1/2010 on the concepts of "controller" and "processor"* (WP 169, 16 February 2010)

Article 29 Data Protection Working Party, *Opinion 2/2010 on online behavioural advertising* (WP 171, 22 June 2010)

Article 29 Data Protection Working Party, *Opinion 3/2010 on the Principle of Accountability* (WP 173, 13 July 2010)

Article 29 Data Protection Working Party, *Opinion 13/2011 on Geolocation services on smart mobile devices* (WP185, 16 May 2011)

Article 29 Data Protection Working Party, *Opinion 15/2011 on the Definition of Consent* (WP187, 13 July 2011)

Article 29 Data Protection Working Party, *Opinion 02/2013 on apps on smart devices* (WP 202, 27 February 2013)

Article 29 Data Protection Working Party, *Opinion 03/2013 on Purpose Limitation* (WP 203, 2 April 2013)

Article 29 Data Protection Working Party, *Working Document 02/2013 Providing Guidance on Obtaining Consent for Cookies* (WP 208, 2 October 2013)

Article 29 Data Protection Working Party, *Opinion 06/2014 on the Notion of Legitimate Interests of the Data Controller under Article 7 of Directive 95/46/EC* (WP 217, 9 April 2014)

Article 29 Data Protection Working Party, *Statement on the Role of a Risk-based Approach in Data Protection Legal Framework* (WP 218, 30 May 2014)

Article 29 Data Protection Working Party, *Statement on the impact of the development of big data on the protection of individuals with regard to the processing of their personal data in the EU* (WP 221, 16 September 2014)

Article 29 Data Protection Working Party, *Guidelines on Data Protection Officers ('DPOs')* (WP 243 rev01, 13 December 2016, last revised 5 April 2017)

Article 29 Data Protection Working Party, *Guidelines on Data Protection Impact Assessment (DPIA) and Determining Whether Processing is "Likely to Result in a High Risk" for the*

Purposes of Regulation 2016/679 (WP 248 rev01, 4 April 2017, last revised October 2017)

Article 29 Data Protection Working Party, *Guidelines on Consent under Regulation 2016/679* (WP 259, 28 November 2017)

Article 29 Data Protection Working Party, *Guidelines on Automated Individual Decision-making and Profiling for the Purposes of Regulation 2016/679* (WP251, rev01, 3 October 2017, last revised 6 February 2018)

European Data Protection Board

European Data Protection Board, *Guidelines 3/2018 on the Territorial Scope of the GDPR (Article 3) - Version for Public Consultation* (16 November 2018)

European Data Protection Board, *Opinion 4/2018 on the draft List of the Competent Supervisory Authority of Czech Republic regarding the Processing Operations subject to the Requirement of a Data Protection Impact Assessment (Article 35.4 GDPR)* (25 September 2018)

European Data Protection Board, *Opinion 5/2019 on the Interplay between the ePrivacy Directive and the GDPR, in particular regarding the Competence, Tasks and Powers of Data Protection Authorities* (12 March 2019)

European Data Protection Board, *Opinion 14/2019 on the draft Standard Contractual Clauses submitted by the DK SA (Article 28(8) GDPR)* (9 July 2019)

European Data Protection Board, *Guidelines 4/2019 on Article 25 Data Protection by Design and by Default* (13 November 2019)

European Data Protection Supervisor

European Data Protection Supervisor (EDPS), *Opinion of the European Data Protection Supervisor on the Communication from the Commission to the European Parliament and the Council on the follow-up of the Work Programme for better implementation of the Data Protection Directive* (2007/C 255/01, 2007)

European Data Protection Supervisor (EDPS), *Opinion of the European Data Protection Supervisor on the communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on 'Radio Frequency Identification (RFID) in Europe: steps towards a policy framework'* (COM(2007) 96 (2008/C 101/01), 2007)

European Data Protection Supervisor (EDPS), *Opinion of the European Data Protection Supervisor on Promoting Trust in the Information Society by Fostering Data Protection and Privacy* (2010)

European Data Protection Supervisor (EDPS), *Opinion of the European Data Protection Supervisor on the Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions - "A comprehensive approach on personal data protection in the European Union"* (2011)

European Data Protection Supervisor (EDPS), *Privacy and Competitiveness in the Age of Big Data: The Interplay between Data Protection, Competition Law and Consumer Protection in the Digital Economy* (2014)

European Data Protection Supervisor (EDPS), *Opinion 8/2016 on the Coherent Enforcement of Fundamental Rights in the Age of Big Data* (2016)

European Data Protection Supervisor (EDPS), *Opinion on the Proposal for a Regulation on Privacy and Electronic Communications (ePrivacy Regulation)* (2017)

European Data Protection Supervisor (EDPS), *Opinion 5/2018 Preliminary Opinion on Privacy by Design* (2018)

United Kingdom Information Commissioner's Office

Information Commissioner's Office (UK), *Privacy by Design* (2008)

Information Commissioner's Office (UK), *Privacy in Mobile Apps: Guidance for App Developers* (2013)

Information Commissioner's Office (UK), *The Right to be Informed* (2018)

Information Commissioner's Office (UK), *Examples of Processing "Likely to Result in High Risk"* (2019)

Information Commissioner's Office (UK), *Guide to the General Data Protection Regulation (GDPR)* (2019)

Information Commissioner's Office (UK), *Update Report into AdTech and Real Time Bidding* (2019)

Other

Data Protection Authority (Belgium), *List of the Types of Processing Operations for which a DPIA shall be Required (Section 35 (4) of the GDPR)* (2019)

Datatilsynet (Danish Data Protection Agency), *DK SA Standard Contractual Clauses for the Purposes of Compliance with Art. 28 GDPR* (2019)

Icelandic Data Protection Authority, *Notice on Processing Operations Subject to the Requirement of a Data Protection Impact Assessment* (2019)

Office for Personal Data Protection of the Czech Republic (UOOU), List *of Processing Operations Subject to Data Protection Impact Assessment* (2019)

Office of the Australian Information Commissioner, *Mobile privacy: A better practice guide for mobile app developers* (2014)

Office of the Privacy Commissioner for Personal Data Hong Kong, *Personal data privacy protection: what mobile apps developers and their clients should know* (2012)

Dissertations

Almuhimedi H, 'Helping Smartphone Users Manage their Privacy through Nudges' (DPhil, Carnegie Mellon 2017)

Andow BE, 'Privacy Risks of Sensitive User Data Exposure in Mobile Ecosystems' (DPhil (Computer Science), North Carolina State University 2019)

Bhana D, 'Constitutionalising contract law: Ideology, judicial method and contractual autonomy' (DPhil Wits 2013)

Evans HW, 'Corporate social responsibility (CSR): tailoring regulation and government policy to the needs of small and medium-sized enterprises' (2017)

Karegar F, 'Towards Improving Transparency, Intervenability, and Consent in HCI' (Karlstad University Press 2018)

Liu B, 'Can Machine Learning Help People Configure Their Mobile App Privacy Settings?' (DPhil Carnegie Mellon 2019)

Liu Y, 'User Data Sharing in Online Services' (Northeastern University 2016)

London RW, 'Comparative data protection and security law: A critical evaluation of legal standards' (University of South Africa 2013)

Pham TVA, *Privacy-Enhancing Technologies for Mobile Applications and Services* (D. Sc. Ecole polytechnique fédérale de Lausanne (EPFL), 2019)

Ren J, 'Measuring Personal Information Exposure in the Mobile and IoT Environments' (Northeastern University 2019)

Roos A, 'The law of data (privacy) protection: a comparative and theoretical study' (UNISA 2009)

Swales L, 'An analysis of the regulatory environment governing electronic evidence in South Africa: suggestions for reform' (UCT 2019).

Townsend BA, ‘Privacy and data protection in eHealth in Africa-an assessment of the regulatory frameworks that govern privacy and data protection in the effective implementation of electronic health care in Africa: is there a need for reform and greater regional collaboration in regulatory policymaking?’ (University of Cape Town 2017)

Ullah I, ‘Privacy-preserving mechanisms for targeted mobile advertising’ (University of New South Wales, Sydney, Australia 2017)

Van der Maelen C, ‘Digital Privacy Protection Against Corporate Actors in the European Union: Benefits, Flaws and Repercussions’ (Masters thesis, Ghent University 2017)

Xu M, ‘A System Perspective to Privacy, Security and Resilience in Mobile Applications’ (University of Saskatchewan 2019)

Internet Sources

‘Ad Exchange’ <https://en.wikipedia.org/wiki/Ad_exchange> accessed 24 Oct 2019

Afonin O, ‘Android Encryption Demystified’ (23 May 2017) <https://blog.elcomsoft.com/2017/05/android-encryption-demystified/> accessed 19 February 2020

African Union ‘List of countries which have signed, ratified/acceded to the African Union Convention on Cyber Security and Personal Data Protection’ (18 June 2020) < https://au.int/sites/default/files/treaties/29560-sl-african%20union%20convention%20on%20cyber%20security%20and%20personal%20data%20protection.pdf> accessed 1 August 2020.

allaboutcookies.org, ‘Mobile technology tracking methods other than cookies’ <https://www.allaboutcookies.org/mobile/mobile-tracking.html> accessed 3 November 2019

Android Developers, ‘Android 8.0 Behavior Changes’ <https://developer.android.com/about/versions/oreo/android-8.0-changes> accessed 19 February 2020

Android, ‘Android PlayProtect’ <https://www.android.com/play-protect/>

Android Developers, ‘Background Execution Limits’ (27 December 2019) https://developer.android.com/about/versions/oreo/background#broadcasts accessed 19 February 2020

Android Developers, ‘Background Location Limits’ https://developer.android.com/about/versions/oreo/background-location-limits.html accessed 19 February 2020

Android Developers, ‘Best Practices for Unique Identifiers’ <https://developer.android.com/training/articles/user-data-ids> accessed 26 February 2020

Android Developers, ‘Broadcasts Overview’ <https://developer.android.com/guide/components/broadcasts> accessed 19 February 2020

Android Developers, ‘Guide to Background Processing’ (27 December 2019) <https://developer.android.com/guide/background> accessed 19 February 2020

Android Developers, ‘Implicit Broadcast Exceptions’ https://developer.android.com/guide/components/broadcast-exceptions.html accessed 19 February 2020

Android Developers, ‘Launch checklist’ (27 December 2019) https://developer.android.com/distribute/best-practices/launch/launch-checklist accessed 9 April 2020

Android Developers, ‘Notifications Overview’ (27 December 2019) <https://developer.android.com/guide/topics/ui/notifiers/notifications> accessed 13 April 2020

Android Developers, ‘Permissions Overview’ <https://developer.android.com/guide/topics/permissions/overview#dangerous_permissions> accessed 31 August 2019

Android Developers, ‘Privacy best practices’ (27 December 2019) <https://developer.android.com/privacy/best-practices> accessed 19 February 2020

Android Developers, ‘Privacy changes in Android 10’ (27 December 2019) <https://developer.android.com/about/versions/10/privacy/changes> accessed 19 February 2020

Android Developers, ‘Security with HTTPS and SSL’ (27 December 2019) <https://developer.android.com/training/articles/security-ssl> accessed 27 February 2020

APEC, ‘List of APEC member states’ <https://www.apec.org/About-Us/About-APEC/Member-Economies.aspx> accessed 26 October 2019

‘App Privacy Policy Generator’ <https://app-privacy-policy-generator.firebaseapp.com/> accessed 16 May 2019

AppAnnie, ‘The State of Mobile 2019’ (2018) <https://www.appannie.com/en/go/state-of-mobile-2019/> accessed 15 May 2020

Apple, ‘Categories and Discoverability - App Store - App Developer’ <https://developer.apple.com/app-store/categories/> accessed 16 May 2019

Apple, ‘App Store Guidelines’ (12 September 2019) <https://developer.apple.com/app-store/review/guidelines/> accessed 28 February 2020

Apple, ‘App store review guidelines’ (19 December 2018) <https://developer.apple.com/app-store/review/guidelines/#metadata/> accessed 16 May 2019

Apple Developer Centre, ‘Preventing Insecure Network Connections’ <https://developer.apple.com/documentation/security/preventing_insecure_network_connections> accessed 27 February 2020

Apple Developer Centre, ‘Requesting Permission’ <https://developer.apple.com/design/human-interface-guidelines/ios/app-architecture/requesting-permission/> accessed 31 August 2019

Apple Developer Centre, ‘Security’ <https://developer.apple.com/security/> accessed 27 February 2020

Apple Developer Centre, ‘CNCopyCurrentNetworkInfo’ (2020) <https://developer.apple.com/documentation/systemconfiguration/1614126-cncopycurrentnetworkinfo> accessed 8 March 2020

Apple Inc., ‘Apple Developer Agreement’ <https://developer.apple.com/terms/apple-developer-agreement/Apple-Developer-Agreement-English.pdf> accessed 24 Oct 2019

Apple Inc., ‘Apple Privacy Policy’ (29 August 2019) <https://www.apple.com/legal/privacy/en-ww/> accessed 26 October 2019

Apple Inc., ‘Transparency Report’ (2018) <https://www.apple.com/legal/transparency/> accessed 26 October 2019

Association for Competitive Technology (ACT) The App Association, ‘App Privacy and Transparency’ <https://actonline.org/privacy/> accessed 2 March 2020

Association for Competitive Technology (ACT) The App Association, ‘Privacy Dashboard’ <https://actonline.org/projects/privacy-dashboard/> accessed 2 March 2020

Berners-Lee’ (4 October 2018) <https://khanna.house.gov/media/press-releases/release-rep-khanna-releases-internet-bill-rights-principles-endorsed-sir-tim> accessed 25 February 2020

Bischoff P, ‘What is the Consumer Privacy Bill of Rights?’ (27 November 2018) https://www.comparitech.com/blog/vpn-privacy/consumer-privacy-bill-of-rights/ accessed 25 February 2020

Board of Governors of the Federal Reserve System and others, 'Final Model Privacy Notice Form' (17 November 2009) https://www.sec.gov/news/press/2009/2009-248.htm accessed 18 February 2020

Buchman K, 'Study: Internet User Adoption of DNT Hard to Predict' (20 March 2012) <https://www.adweek.com/digital/study-internet-user-adoption-dnt-hard-predict-139091/> accessed 4 March 2020

Burns H, 'How To Protect Your Users With The Privacy By Design Framework' (27 July 2017) <https://www.smashingmagazine.com/2017/07/privacy-by-design-framework/> accessed 26 October 2019

California Department of Justice, 'Privacy Laws' (2019) <https://oag.ca.gov/privacy/privacy-laws> accessed 12 September 2019

'Cambridge English Dictionary' <https://dictionary.cambridge.org/dictionary/english/> accessed 30 March 2020

Cavoukian A, 'Privacy by design: The global privacy standard' (16 October 2018) <https://www.standardsuniversity.org/e-magazine/october-2018-volume-9-issue-3-privacy-freedom-human-rights/privacy-by-design-the-global-privacy-standard/> accessed 24 February 2020

Cavoukian A, 'Privacy by Design: The 7 Foundational Principles' (2009 (revised January 2011)) <https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf> accessed 26 September 2019

Centre for Democracy and Technology, 'Mobile platforms as intermediaries: Liability protections in the United States, the European Union, and Canada' (27 September 2012) <https://cdt.org/wp-content/uploads/pdfs/Mobile-Platforms-As-Intermediaries.pdf> accessed 16 March 2020

Clements J, 'Distribution of worldwide mobile application revenues in 2017, by channel' (20 Feb 2018) <https://www.statista.com/statistics/273120/share-of-worldwide-mobile-app-revenues-by-channel/> accessed 24 Oct 2019

Corfield G, 'TfL to track Tube users in stations by their MAC addresses' (27 November 2016) <https://www.theregister.co.uk/2016/11/17/tfl_to_track_tube_users_by_wifi_device_mac_address/> accessed 26 February 2020

Council of Europe, ‘Chart of signatures and ratifications of Treaty 108’ <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/signatures?p_auth=783d1rIE> accessed 1 June 2019

Council of Europe, ‘Our Member States’ <https://www.coe.int/en/web/about-us/our-member-states> accessed 1 June 2019

Cox J, ‘Zoom is Leaking Peoples' Email Addresses and Photos to Strangers’ (Vice Tech, 1 April 2020) <https://www.vice.com/en_us/article/k7e95m/zoom-leaking-email-addresses-photos> accessed 4 April 2020

Cox J, ‘Zoom iOS App Sends Data to Facebook Even if You Don’t Have a Facebook Account’ (Vice Tech, 26 March 2020) <https://www.vice.com/en_us/article/k7e599/zoom-ios-app-sends-data-to-facebook-even-if-you-dont-have-a-facebook-account> accessed 4 April 2020

Cronje D, ‘Quick guide to introducing AI to your company’ https://www.offerzen.com/blog/quick-guide-introducing-AI-to-your-company accessed 17 May 2019

Data Protection Commission Ireland, ‘Data Protection Commission launches Statutory Inquiry into Google’s processing of location data and transparency surrounding that processing’ (4 February 2020) <https://www.dataprotection.ie/en/data-protection-commission-launches-statutory-inquiry-googles-processing-location-data-and> accessed 26 February 2020

Data Protection Commission Ireland, ‘Data Protection Commission opens statutory inquiry into Google Ireland Limited’ (22 May 2019) <https://www.dataprotection.ie/en/news-media/press-releases/data-protection-commission-opens-statutory-inquiry-google-ireland-limited> accessed 26 February 2020

‘Difference Between App and Widget’ (11 April 2018) <http://www.differencebetween.net/technology/difference-between-app-and-widget/> accessed 6 March 2020

Dogtiev A, ‘Mobile App Developer Statistics Roundup’ ‘https://www.businessofapps.com/news/mobile-app-developer-statistics-roundup/’ (20 January 2016) <https://www.businessofapps.com/news/mobile-app-developer-statistics-roundup/> accessed 28 February 2020

Dooley D, ‘Putting TLS Pinning in Your Mobile Apps’ (*Infosecurity Magazine*, 26 October 2018) https://www.infosecurity-magazine.com/opinions/tls-pinning-mobile-apps/ accessed 27 February 2020

‘Downloading Region Restricted Apps on Android’ (1 March 2019) https://hide.me/en/knowledgebase/downloading-region-restricted-apps-on-android/ accessed 13 March 2020

ElHady H, ‘Guide to Mobile App Analytics’ <https://instabug.com/blog/mobile-app-analytics/> accessed 26 October 2019

Emeis R, ‘Preliminary Report from the 10-City Application Developers Alliance Privacy Summit Series’ (29 November 2012) <https://www.developersalliance.org/press-releases/preliminary-report-from-the-10-city-application-developers-alliance-privacy-summit-series> accessed 2 March 2020

‘Equifax Data Breach Settlement’ <https://www.equifaxbreachsettlement.com/> accessed 26 February 2020

European Data Protection Board, ‘Register for Decisions taken by supervisory authorities and courts on issues handled in the consistency mechanism’ <Register for Decisions taken by supervisory authorities and courts on issues handled in the consistency mechanism> accessed 19 March 2020

European Data Protection Supervisor, ‘Glossary 'Privacy by Design'’ <https://edps.europa.eu/node/3110#privacy_by_design> accessed 17 February 2020

Facebook for developers, ‘Changelog archive’ <https://developers.facebook.com/docs/graph-api/changelog/archive/> accessed 26 February 2020

Facebook Inc., ‘Facebook Platform Policy’ <https://developers.facebook.com/policy/> accessed 26 October 2019

Facebook Inc., ‘Data Policy’ (19 April 2018) <https://www.facebook.com/about/privacy> accessed 26 October 2019

‘Farag v Kiip Settlement’ <https://www.kiipsettlement.com/> accessed 26 February 2020

Federal Trade Commission, ‘Complying with COPPA: Frequently Asked Questions’ <https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions> accessed 8 March 2020

Federal Trade Commission, ‘COPPA Safe Harbour Program’ <https://www.ftc.gov/safe-harbor-program> accessed 4 March 2020

Federal Trade Commission, ‘Student Privacy and Ed Tech’ (1 December 2017) https://www.ftc.gov/news-events/events-calendar/2017/12/student-privacy-ed-tech accessed 5 March 2020

Federal Trade Commission, ‘Protecting Children's Privacy Under COPPA ’ (*Video,* 1 July 2013) <https://www.ftc.gov/news-events/audio-video/video/protecting-childrens-privacy-under-coppa> accessed 15 May 2020

Federal Trade Commission, ‘Mobile health app developers: FTC best practices’ (4 April 2016) <https://www.ftc.gov/tips-advice/business-center/guidance/mobile-health-app-developers-ftc-best-practices> accessed 2 March 2020

Federal Trade Commission, ‘Statement of Joseph J. Simons & Christine S. Wilson RegardingFTC and People of the State of New York v. Google LLC and YouTube, LLC ’ (4 September 2019) <https://www.ftc.gov/system/files/documents/public_statements/1542922/simons_wilson_google_youtube_statement.pdf> accessed 15 May 2020

Federal Trade Commission, Commissioner Wilson CS, ‘The FTC’s Role in Supporting Online Safety ’ (Remarks at the Family Online Safety Institute, Washington DC, 21 November 2019) <https://www.ftc.gov/system/files/documents/public_statements/1557684/commissioner_wilson_remarks_at_the_family_online_safety_institute_11-21-19.pdf> accessed 9 March 2020

‘FedRAMP’ <https://www.fedramp.gov/> accessed 22 February 2020

Feller L, ‘Mobile App Retargeting: Benefits and Best Practices’ (*Branch*, 22 March 2019) <https://blog.branch.io/mobile-app-retargeting-benefits-and-best-practices/> accessed 5 March 2020

ForbrukerRåder (Norwegian Consumer Council), ‘#AppFail’ <https://www.forbrukerradet.no/appfail-en/#> accessed 26 February 2020

‘Free Privacy Policy Generator’ <https://www.freeprivacypolicy.com/free-privacy-policy-generator.php> accessed 16 May 2019

Future of Privacy Forum and Center for Democracy & Technology, ‘Best Practices for Mobile Application Developers’ (12 July 2012) <https://fpf.org/wp-content/uploads/Apps-Best-Practices-v-beta.pdf> accessed 28 February 2020

Gartner IT Glossary, ‘Definition of Big Data’ <https://www.gartner.com/en/information-technology/glossary/big-

data#:~:text=Big%20data%20is%20high%2Dvolume,decision%20making%2C%20and%20process%20automation.> accessed 1 August 2020.

gdad-s-river, 'Metadata: Story Of How Whatsapp And Other Chat Apps Collect Data' (*Fossbytes*, 27 January 2017) <https://fossbytes.com/whatsapp-chats-collect-data-metadata/> accessed 26 October 2019

Gonschorek A, 'How Luno Uses Data to Make Product Decisions' <https://www.offerzen.com/blog/how-luno-uses-data-to-make-product-decisions> accessed 17 May 2019

Gonschorek A, 'Up in the Cloud - Hyrax Revolutionises Drug-Resistance-Testing' <https://www.offerzen.com/blog/up-in-the-cloud-hyrax-revolutionises-drug-resistance-testing> accessed 17 May 2019

Google, 'Google Play Developer Policy Centre' <https://play.google.com/intl/en-US/about/developer-content-policy-print/> accessed 24 Oct 2019

Google, 'Privacy, Security, and Deception' <https://play.google.com/about/privacy-security-deception/personal-sensitive/> accessed 16 May 2019

Google, 'Select a category for your app or game' https://support.google.com/googleplay/android-developer/answer/113475?hl=en accessed 16 May 2019

Google, 'Google Play Developer Distribution Agreement' (15 April 2019) <https://play.google.com/about/developer-distribution-agreement.html> accessed 24 Oct 2019

Google, 'Google Play Developer Distribution Agreement' (17 November 2020) <https://play.google.com/about/developer-distribution-agreement.html> accessed 8 February 2021

Google, 'Google Controller-Controller Data Protection Terms' < https://privacy.google.com/businesses/gdprcontrollerterms/> accessed 8 February 2021

Google, 'Google Controller-Controller Data Protection Terms: Standard Contractual Clauses; SET II - Standard contractual clauses for the transfer of personal data from the Community to third countries (controller to controller transfers)' '<https://privacy.google.com/businesses/gdprcontrollerterms/sccs/> accessed on 8 February 2021

Google Ad Manager, 'Mobile Ads SDK Android Guide' <https://developers.google.com/ad-manager/mobile-ads-sdk/android/quick-start> accessed 24 Oct 2019

Google Ad Manager Help, ‘How mobile app interstitials work’ <https://support.google.com/admanager/answer/6015986?hl=en> accessed 24 Oct 2019

Google Inc., ‘Transparency Report’ (2019) <https://transparencyreport.google.com/?hl=en> accessed 26 October 2019

Google LLC., ‘How Google shows you ads’ <adssettings.google.com> accessed 3 November 2019

Google LLC., ‘Mobile app backend services’ (13 May 2019) <https://cloud.google.com/solutions/mobile/mobile-app-backend-services> accessed 26 October 2019

Google LLC., ‘Google Privacy Policy’ (15 Oct 2019) <https://www.gstatic.com/policies/privacy/pdf/20191015/9ad23b47/google_privacy_policy_en.pdf> accessed 24 Oct 2019

Google LLC., ‘Google Terms of Service’ (25 Oct 2017) <https://policies.google.com/terms?hl=en&gl=us> accessed 24 Oct 2019

Google Play Console Help, ‘Advertising ID’ <https://support.google.com/googleplay/android-developer/answer/6048248?hl=en> accessed 24 Oct 2019

Google Play Developer Policy Centre, ‘Advertising ID ’ https://play.google.com/about/monetization-ads/ads/#!?zippy_activeEl=ad-id#ad-id accessed 24 Oct 2019

Google Play Developer Policy Centre, ‘Permissions’ <https://play.google.com/about/privacy-security-deception/permissions/> accessed 31 August 2019

GSM Arena, ‘All Mobile Phone Brands’ <https://www.gsmarena.com/makers.php3> accessed 24 Oct 2019

Help GAM, ‘Rewarded inventory policy’ <https://support.google.com/admanager/answer/7496282> accessed 24 Oct 2019

Higgins P, ‘A Better Path for Apps: Respecting Users and Their Privacy’ (*Electronic Frontier Foundation,* 8 February 2012) <https://www.eff.org/deeplinks/2012/02/better-path-apps-respecting-users-and-their-privacy> accessed 6 March 2020

Hill K, ‘Data Broker Was Selling Lists Of Rape Victims, Alcoholics, and 'Erectile Dysfunction Sufferers'’ (19 December 2013) <https://www.forbes.com/sites/kashmirhill/2013/12/19/data-broker-was-selling-lists-of-

rape-alcoholism-and-erectile-dysfunction-sufferers/#6ab63ca71d53> accessed 26 October 2019

International Association of Privacy Professionals (IAPP) Westin Research Centre, 'Comparison of Mobile Applications Guidelines' <https://iapp.org/resources/comparison-of-mobile-application-guidelines/> accessed 2 March 2020

International Council on Systems Engineering (INCOSE), 'What is Systems Engineering?' (2019) <https://www.incose.org/systems-engineering> accessed 29 September 2019

International Electrotechnical Commission (IEC), 'Digital Technology-Fundamental Concepts' <http://www.electropedia.org/iev/iev.nsf/index?openform&part=171> accessed 9 April 2020

International Telecommunications Union (ITU), 'Telecommunication Terminology Database (TERMITE)' <https://www.itu.int/pub/S-TERM-DB> accessed 16 May 2020

ISO, ''Technical Committees'' <https://www.iso.org/technical-committees.html> accessed 3 March 2020

Iuebenda.com, 'Iuebenda Privacy Policy Generator' <www.iubenda.com/> accessed 15 May 2020

Jacobs J, 'A Message to Our Users ' (*Runkeeper Blog*, 17 May 2016) <http://blog.runkeeper.com/4714/a-message-toour-users/> accessed 26 February 2020

Jin GZ and Stivers A, 'Protecting Consumers in Privacy and Data Security: A Perspective of Information Economics' [2017]<https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3006172> accessed 15 May 2020

Juniper Networks, 'Understanding the Network Terms BSSID, SSID and ESSID' (5 October 2018) <https://www.juniper.net/documentation/en_US/junos-space-apps/network-director3.7/topics/concept/wireless-ssid-bssid-essid.html> accessed 8 March 2020

Kangin L, 'Interview with Brian Wong' (*Brief Communications Inc*, 2019) <https://gobrief.com/interviews/kiip-with-brian-wong/> accessed 15 May 2020

Kaspersky, 'iPhone Encryption: How to Encrypt Your iPhone' https://usa.kaspersky.com/resource-center/preemptive-safety/iphone-encryption accessed 19 February 2020

Khanna R, 'Rep. Khanna releases 'Internet Bill of Rights' principles, endorsed by Sir Tim

Kuan HH, ‘GDPR: Killing cloud quickly?’ (*International Association of Privacy Professsionals (IAPP),* 17 March 2016) <https://iapp.org/news/a/gdpr-killing-cloud-quickly/> accessed 7 March 2018

‘List of mobile app distribution platforms’ (20 Sept 2019) <https://en.wikipedia.org/wiki/List_of_mobile_app_distribution_platforms> accessed 24 Oct 2019

Lizar M and Pandit HJ, ‘OPN: Open Notice Receipt Schema’ (2019) <http://ceur-ws.org/Vol-2451/paper-21.pdf> accessed 24 February 2020

Manolo A, ‘Change Your App Store Country to Download Region-Locked Apps & Games on Your iPhone’ (21 March 2017) <https://ios.gadgethacks.com/how-to/change-your-app-store-country-download-region-locked-apps-games-your-iphone-0176591/> accessed 13 March 2020

Martin J and others, ‘Handoff All Your Privacy: A Review of Apple's Bluetooth Low Energy Implementation’ [2019] <arXiv preprint arXiv:1904.10600> accessed 15 May 2020

Mahieu R and van Hoboken J, ‘Fashion-ID: Introducing a Phase oriented Approach to Data Protection?’ *European Law Blog* (30 September 2019) <https://europeanlawblog.eu/2019/09/30/fashion-id-introducing-a-phase-oriented-approach-to-data-protection/> accessed 15 August 2020.

Mayer J, ‘Safari Trackers’ (17 February 2012) <http://webpolicy.org/2012/02/17/safari-trackers/> accessed 26 February 2020

Milkaite I and Lievens E, ‘The GDPR child's age of consent for data processing across the EU – one year later (July 2019)’ (1 July 2019) <https://www.betterinternetforkids.eu/web/portal/practice/awareness/detail?articleId=3017751> accessed 22 August 2019

Mucheru, H.E. Joseph, ‘Using tech to 'leapfrog' Kenya's development challenges: H.E. Joseph Mucheru (interview) ’ (ITU Plenipotentiary Conference, Dubai, 29 October - 16 November 2018)

Nakashima R, ‘Google tracks your movements, like it or not’ (*Associated Press,* 14 August 2018) <https://apnews.com/828aefab64d4411bac257a07c1af0ecb> accessed 14 April 2020

National Association of Criminal Defense Lawyers (NACDL), ‘Cell Phone Location Tracking’ <https://www.law.berkeley.edu/wp-content/uploads/2015/04/2016-06-07_Cell-Tracking-Primer_Final.pdf> accessed 26 July 2019

National Conference of State Legislatures (NCSL), '2019 Consumer Data Privacy Legislation' (2019) <https://www.ncsl.org/research/telecommunications-and-information-technology/consumer-data-privacy.aspx> accessed 25 February 2020

Netapp, 'Object Storage vs. File Storage vs. Block Storage' <https://www.netapp.com/us/info/what-is-object-storage.aspx> accessed 13 April 2020

Network Advertising Initiative (NAI), 'The NAI Code of Conduct' (2020) <https://www.networkadvertising.org/code-enforcement/code> accessed 2 March 2020

New York Attorney General, 'A.G. Schneiderman Announces Settlement with Uber to Enhance Rider Privacy' (6 January 2016) <https://ag.ny.gov/press-release/2016/ag-schneiderman-announces-settlement-uber-enhance-rider-privacy> accessed 2 March 2020

New York Attorney General, 'A.G. Underwood Announces Record $148 Million Settlement With Uber Over 2016 Data Breach ' (26 September 2018) <https://ag.ny.gov/press-release/2018/ag-underwood-announces-record-148-million-settlement-uber-over-2016-data-breach> accessed 2 March 2020

Newton L, 'GPEN Sweep 2018 - International investigation finds that organisations should be doing more to achieve privacy accountability' (*Global Privacy Enforcement Network,,* 5 March 2019) <https://privacyenforcement.net/press-releases> accessed 04 April 2020

NinthDecimal, 'Consumer and Data Privacy' <https://www.ninthdecimal.com/> accessed 26 February 2020

NIST, 'FIPS' <https://csrc.nist.gov/publications/fips> accessed 26 October 2019

OASIS, 'OASIS Privacy by Design Documentation for Software Engineers (PbD-SE) TC' <https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=pbd-se> accessed 2 March 2020

OECD, 'Glossary of Statistical Terms' <https://stats.oecd.org/glossary/detail.asp?ID=68> accessed 4 April 2020

OECD, 'List of OECD Member countries - Ratification of the Convention on the OECD' <https://www.oecd.org/about/document/list-oecd-member-countries.htm> accessed 26 October 2019

Office of the Privacy Commissioner of Canada, 'Guidelines for Obtaining Meaningful Consent' (May 2018) <https://www.priv.gc.ca/en/privacy-topics/collecting-personal-information/consent/gl_omc_201805/> accessed 18 February 2020

Office of the Privacy Commissioner of Canada, 'Ten tips for communicating your app's privacy practices to your app's users' (September 2014)

<https://www.priv.gc.ca/en/privacy-topics/technology/mobile-and-digital-devices/mobile-apps/02_05_d_61_tips/> accessed 18 February 2020

Payment Card Industry (PCI) Security Standards Council, 'Migrating from SSL and Early TLS A Resource Guide from the PCI Security Standards Council' (2018) <https://www.pcisecuritystandards.org/pdfs/PCI_SSC_Migrating_from_SSL_and_Early_TLS_Resource_Guide.pdf?agreement=true&time=1582791832037> accessed 27 February 2020

PayPal Developer, 'Get started with mobile payment libraries' (2020) <https://developer.paypal.com/docs/archive/mobile/gs_MPL/> accessed 27 February 2020

Pell RR, 'Third-Party Data Collection and Consent in Mobile Applications' (16 January 2019) <https://info.dechert.com/10/11731/january-2019/2019-01-15-third-party-data-collection-and-consent-in-mobile-applications.asp?sid=e3e7d5f3-d44e-4edc-93d5-0e787cb84a28#> accessed 25 April 2019

Privacy International, 'Why we've filed complaints against companies that most people have never heard of – and what needs to happen next' (8 November 2018) <https://privacyinternational.org/advocacy/2434/why-weve-filed-complaints-against-companies-most-people-have-never-heard-and-what> accessed 26 October 2019

'PrivacyChoice' <https://www.privacychoice.org> accessed 16 May 2019

Priyadarshini M, 'Which Sensors Do I Have In My Smartphone? How Do They Work?' (25 Sept 2018) <https://fossbytes.com/which-smartphone-sensors-how-work/> accessed 29 October 2019

Razaghpanah A and others, 'Apps, trackers, privacy, and regulators: A global study of the mobile tracking ecosystem' [2018] <https://www.ftc.gov/system/files/documents/public_comments/2018/08/ftc-2018-0052-d-0036-154997.pdf> accessed 29 October 2019

Reding V, 'Privacy: the Challenges Ahead for the European Union; Keynote Speech at the Data Protection Day' (*European Parliament,* 28 January 2010) <https://europa.eu/rapid/press-release_SPEECH-10-16_en.htm> accessed 28 September 2019

Riley J, 'Understanding Metadata: What is Metadata, and What is it For?: A Primer' (*National Information Standards Organisation (NISO),* 2017)

<https://www.niso.org/publications/understanding-metadata-2017> accessed 26 October 2019

Ryan J, 'Report from Dr Johnny Ryan – Behavioural advertising and personal data' (5 September 2018) <https://brave.com/wp-content/uploads/Behavioural-advertising-and-personal-data.pdf> accessed 26 February 2020

Schema.org, 'Schema v6.0' <https://schema.org/docs/releases.html> accessed 24 February 2020

Schiff A, 'Mobile Device IDs Will Be The Next Ad Tracker To Bite The Dust' (10 February 2020) <https://www.adexchanger.com/mobile/mobile-device-ids-will-be-the-next-ad-tracker-to-bite-the-dust/> accessed 22 April 2020

Schwab K, 'The Fourth Industrial Revolution: what it means and how to respond' (*World Economic Forum,* 14 Jan 2016) <https://www.weforum.org/agenda/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond> accessed 24 July 2018

Scott Brown C, '80% of Android apps are encrypting traffic by default, up from 0% in early 2018' (*StackExchange,* 3 December 2019) <https://www.androidauthority.com/android-app-encryption-1062202/> accessed 27 February 2020

Snigdha, '25 Best Programming Languages for Mobile Apps & Top Mobile App Development Tools & Frameworks' (18 Sept 2019) <https://www.appypie.com/app-development-guide> accessed 24 October 2019

Statcounter, 'Mobile Operating System Market Share Worldwide' <https://gs.statcounter.com/os-market-share/mobile/worldwide> accessed 24 October 2019

Sutherland E, 'Digital Privacy in Africa: Cybersecurity, Data Protection & Surveillance' [2018] < http://dx.doi.org/10.2139/ssrn.3201310> accessed 18 April 2020

Swaroop S, 'How to fix Advertising ID policy violation in Google Play Store really quick?' (25 Sept 2018) <https://blog.usejournal.com/how-to-fix-advertising-id-policy-violation-in-google-play-store-6d9cf92d335d> accessed 24 Oct 2019

Taplytics, 'App Personalization: The 5 Best Personalized Apps' (28 March 2019) <https://taplytics.com/blog/app-personalization-5-best-personalized-apps/> accessed 4 March 2020

Techopedia, 'Data Synchronisation' <https://www.techopedia.com/definition/1006/data-synchronization> accessed 13 April 2020

Techopedia, ‘Geotagging’ <https://www.techopedia.com/definition/86/geotagging> accessed 25 February 2020

Techopedia, ‘Scalability’ <https://www.techopedia.com/definition/9269/scalability> accessed 13 April 2020

Techopedia, ‘What does crash mean?’ <https://www.techopedia.com/definition/13399/crash> accessed 13 April 2020

Techopedia, ‘What is a query?’ <https://www.techopedia.com/definition/5736/query> accessed 13 April 2020

Techopedia, ‘What is an avatar?’ <https://www.techopedia.com/definition/4624/avatar> accessed 13 April 2020

Techopedia, ‘What is raw data?’ <https://www.techopedia.com/definition/1230/raw-data> accessed 13 April 2020

TermsFeed, ‘CalOppa: Your Guide to Creating a Compliant Privacy Policy’ <https://www.termsfeed.com/blog/caloppa-compliant-privacy-policy/> accessed 9 March 2020

TermsFeed, ‘Privacy Policy Generator’ <https://www.termsfeed.com/privacy-policy-generator/> accessed 2 March 2020

TikTok Inc, ‘Privacy Policy for Younger Users’ (January 2020) <https://www.tiktok.com/legal/privacy-policy-for-younger-users?lang=en> accessed 6 March 2020

TrustArc, ‘Truste Model Privacy Disclosures’ http://chnm.gmu.edu/digitalhistory/links/cached/chapter6/6_24c_disclosures.htm accessed 3 March 2020

‘TRUSTe Assurance ’ <https://www.trustarc.com/> accessed 16 May 2019

‘WebRTC’ <https://webrtc.org/> accessed 4 March 2020

Turrecha L, ‘Americans might be getting a comprehensive federal privacy law soon’ (18 February 2020) <https://medium.com/golden-data/americans-might-be-getting-a-comprehensive-federal-privacy-law-soon-64bc6e03ab94> accessed 25 February 2020

United Nations Conference on Trade and Development (UNCTAD), ‘Digital transformation for all: empowering entrepreneurs and small business (Audio recording of conference proceedings on 25 April 2017)’ (*UNCTAD e-commerce week*, 24-28 April 2017) <http://unctad.org/en/conferences/e-week2017/Pages/MeetingDetails.aspx?meetingid=1318> accessed 10 May 2017

US Department of Commerce, ‘EU-U.S. Privacy Shield Framework Principles’ <https://www.privacyshield.gov/servlet/servlet.FileDownload?file=015t00000004qAg> accessed 1 September 2019

US Department of Commerce, ‘Swiss-US Privacy Shield Framework’ <https://www.trade.gov/td/services/odsi/swiss-us-privacyshield-framework.pdf> accessed 1 September 2019

US Department of Health and Human Services, ‘Health Information Privacy’ <https://www.hhs.gov/hipaa/for-professionals/privacy/index.html> accessed 21 February 2020

US Department of Health and Human Services, ‘Health App Use Scenarios & HIPAA’ (February 2016) <https://hipaaqsportal.hhs.gov/community-library/accounts/92/925889/Public/OCR-health-app-developer-scenarios-2-2016.pdf> accessed 22 February 2020

US Small Business Administration, ‘Table of Size Standards’ (19 August 2019) <https://www.sba.gov/document/support--table-size-standards> accessed 5 March 2020

US Supreme Court, case information in *Oracle America Inc. v Google Inc.* <. https://www.supremecourt.gov/search.aspx?filename=/docket/docketfiles/html/public/18-956.html> accessed 22 July 2020.

White House (Obama Administration), ‘Consumer Privacy Bill of Rights Act 2015 Discussion Draft’ (2015) <https://obamawhitehouse.archives.gov/sites/default/files/omb/legislative/letters/cpbr-act-of-2015-discussion-draft.pdf> accessed 13 May 2020

Wicker R, ‘Chairman's Statement at US Senate Committee on Commerce, Science and Transportation Hearing: Examining Legislative Proposals to Protect Consumer Data Privacy’ (4 December 2019) <https://www.commerce.senate.gov/2019/12/examining-legislative-proposals-to-protect-consumer-data-privacy> accessed 25 February 2020

Wikipedia, ‘Certificate Authority’ <https://en.wikipedia.org/wiki/Certificate_authority> accessed 27 February 2020

Wikipedia, ‘Form Factor (Mobile Phones)’ <https://en.wikipedia.org/wiki/Form_factor_(mobile_phones)> accessed 19 February 2020

Wikipedia, ‘HTTPS’ <https://en.wikipedia.org/wiki/HTTPS#cite_note-6> accessed 27 February 2020

Wikipedia, ‘System on a Chip’ <https://en.wikipedia.org/wiki/System_on_a_chip> accessed 28 February 2020

Wlosik M, ‘What Is a Data Broker and How Does It Work?’ (23 January 2019) <https://clearcode.cc/blog/what-is-data-broker/> accessed 26 October 2019

Wu L, ‘Apps Disguised as Security Tools Bombard Users With Ads and Track Users’ Location’ (3 January 2018) <https://blog.trendmicro.com/trendlabs-security-intelligence/apps-disguised-security-tools-bombard-users-ads-track-users-location/> accessed 28 February 2020

Yuan ES, ‘Zoom’s Use of Facebook’s SDK in iOS Client’ (*Zoom Blog*, 2020) <https://blog.zoom.us/wordpress/2020/03/27/zoom-use-of-facebook-sdk-in-ios-client/> accessed 4 April 2020

Zoom, ‘Privacy Policy’ <https://zoom.us/privacy> accessed 4 April 2020