The Balance between the Data Protection Law Regime and Modern Technologies: Collision or Collaboration? – A Comparative Study of Regulatory Instruments in the EU and Taiwan

WENG, YI-HUNG

The Balance between the Data Protection Law Regime and Modern Technologies: Collision or Collaboration?

− A Comparative Study of Regulatory Instruments in the EU and Taiwan

Yi-Hung Weng

A Thesis submitted for the degree of

Doctor of Philosophy

Durham Law School

Durham University

May 2013

Abstract

The aim of this thesis is to discuss and evaluate how to strike a balance between the benefits and the risks of biometric and Radio-frequency Identification (RFID) technologies within a data protection regime. This presents a problem because of the lack of an applicable theoretical framework and clear guidelines and principles for legal regulations to deal with such technologies. The theory chosen here is the Principle of Generic Consistency (PGC), which has been justified as the basic principle of human rights in any given community.

This thesis then elaborates on specific applications of the PGC in relation to various issues by defining relevant privacy concepts and describing how they are analysed to allow the identification, evaluation, and comparison of competing rights and interests in a specific conflict. Probing and evaluating current regulation of technologies at stake in Europe and Taiwan, it is argued that the right to benefit from advances in science and technology and the right to privacy are bound to come into conflict.

However, it is problematic to suggest that the balancing of competing rights is a zero-sum trade-off. Instead, in line with the broad concept of privacy, it is contended that there is the possibility for the two sets of values to support each other. In this case, the thesis suggests a co-operative framework, which relies on a consistent approach to maintain valid consent, precautionary and preventive measures to tackle the risks of developing such technologies, and an independent institutional framework for personal data protection.

Lastly, the thesis proposes a PGC-derived regulatory framework and model for Taiwan. As the Formosan hydra-headed bureaucracy model generates inconsistent data protection consequences, it is suggested that an institutional framework comprising an independent regulatory body might be able to assist the success of the co-operative model more effectively.

Table of Contents

Statement of Copyright

Acknowledgements

No one would be able to read this thesis had it not been for the generous help and kindness of lots of people around me.

I would like to express my sincerest gratitude to the supervisory team of my doctoral research: Prof. Deryck Beyleveld for his critical but greatly constructive suggestions, quiet but genuine and unfailing support, and, of course, his extraordinary patience with me throughout the entire stage of my research; Prof. Ian Leigh for his valuable insights and wonderful smiles that provided much-needed reassurance. Prof. Graeme Laurie who examined this thesis has offered remarkable feedback, as has Dr Shaun D. Pattinson, who offered continuous encouragement up to the final stages. I am also grateful to my colleague Alice Panepinto for proofreading my thesis when she should have been working on hers.

I would also like to thank to Prof. Fort Fu-Te Liao who led me to pursue academic work in the legal field.

I would like to thank to the Overseas Research Students (ORS) Awards Scheme for the scholarship I have enjoyed for three years.

I would like to extend my special thanks to my colleagues and friends, in particular the ‘PG29 gang’. That little humble research room holds my best ever memories in Durham, where true friendships and a family atmosphere created a pleasant working environment. In that room we shared everything about doing research – joy or frustration. I have enjoyed my time in that workroom greatly, including the ringing from the Durham Cathedral Bells.

Finally, I would like to thank to my family for their crucial support and generous tolerance of my pursuit of academic life.

List of Cases

TAIWAN

J. Y. Interpretation No. 293

J. Y. Interpretation No. 535

J. Y. Interpretation No. 585

J. Y. Interpretation No. 586

J. Y. Interpretation No. 603

J. Y. Interpretation No. 613

J. Y. Interpretation No. 689

THE UNITED KINGDOM

A-G v. Guardian Newspapers (No. 2) [1990] 1 AC 109.

R v Brown and Others [1994] 1 AC 212

Campbell v. MGN [2004] UKHL 22.

Coco v. A. N. Clark (Engineers) Limited [1969] R P C 41, 47.

Derbyshire County Council v Times Newspapers [1992] QB 770.

Derbyshire County Council v Times Newspapers [1993] AC 534.

Durant v Financial Services Authority [2003] EWCA Civ 1746.

Ghaidan v Godin-Mendoza [2004] 2 AC 557, 605

Hellewell v. Chief Constable of Derbyshire [1995] 1 W L R 804, 807.

Johnson v Medical Defence Union [2007] EWCA Civ.

R (on the application of GC) v The Commissioner of Police of the Metropolis [2011] UKSC 21.

R v Chief Constable of South Yorkshire [2002] EWHC 478 (Admin), [2003] EWCA Civ 1275, and [2004] UKHL 39.

R v Department of Health ex p. Source Informatics [1999] 4 All ER 185, [2000] 1 All ER 786.

R v Department of Health ex p. Source Informatics [2001] QB 424.

R v Rooney [2006] EWCA Crim 1841.

R v Secretary of State for the Home Department, ex p Brind [1991] 1 AC 696.

R v Secretary of State for Transport ex parte Faetortame (No 2) [1991]1 AC 603 (HL).

R v Secretary of State for Work and Pensions [2006] 1 AC 173.

R. v. Chief Constable of South Yorkshire [2004] UKHL 39.

R. v. DPP, ex parte Kebilene [2002] 2 AC 326, 380-1.

Rantzen v Mirror Group Newspapers [1994] QB 670, 691.

Regina v. Special Adjudicator ex parte Ullah; Doe v. Secretary of State for the Home Department [2004] UKHL 26.

The College van burgemeester en wethouders van Rotterdam v Rijkeboer Case C-553/07

Thoburn v Sunderland City Council [2003] QB 151.

Wainwright v Home Office [2004] 2 AC 406, [2003] UKHL 53.

EUROPEAN COURT OF JUSTICE

Wagner Miret v Fondo de Guarantia Salaria Case C-334/92 [1993] ECR I-6911.

EUROPEAN COURT OF HUMAN RIGHTS

Airey v Ireland Series A no 32 (1979) 2 EHRR 305.

Amman v Switzerland (App no 27798/95) (2000) 30 EHRR 843.

B v France (1992) 16 EHRR 1.

Bensaid v. the United Kingdom (App no 44599/98) ECHR 2001-I.

Botta v Italy (1998) 26 EHRR 241.

Burghartz v. Switzerland 22 February 1994, Series A no 280-B.

Costello-Roberts v UK (App no 13134/87) (1993) 19 EHRR 112.

Dudgeon v UK (App no 7525/76) (1981) 4 EHRR 149, 165.

Friedl v Austria judgment of 31 January 1995, Series A no 305-B.

Gaskin v UK Series A no 160 (1989) 12 EHRR 36.

Giacomelli v Italy 2006-XII, 45 EHRR 871.

Glass v UK (App no 61827/00) 2004-II 39 EHRR 341.

Goggins and Others v The United Kingdom (App nos 30089/04, 14449/06, 24968/07, 13870/08, 36363/08, 23499/09, 43852/09 and 64027/09).

Guerra v Italy 1998-I, 26 EHRR 357.

Handyside v UK (1976) 1 EHRR 737.

Hatton v UK (2003) 37 EHRR 28.

Hewitt and Harman v UK (App no 12175/86) (1992) 14 EHRR 657 .

Rasmussen v Denmark (1984) 7 EHRR 371.

Rees v UK Series A no 106 (1986) 9 EHRR 56.

Roche v United Kingdom (2006) 42 EHRR 30.

S and Marper v UK (App nos 30562/04 and 30566/04) ECHR 4 (App nos 30562/04 and 30566/04) ECHR 4.

Sciacca v. Italy (App no 50774/99) (2005) ECHR 2005-I.

Sheffield and Horsham v. the United Kingdom (App nos 22985/93; 23390/94) Judgement of 30 July 1998.

Soering v UK Series A161 (App no 14038/88) (1989) 11 EHRR 439.

Ünal Tekeli v. Turkey (App no 29865/96) ECHR 2004-X.

Van der Velden v the Netherlands (App no 29514/05), 7 December 2006.

Vgt Verein Gegen Tierfabriken v. Switzerland Application no 24699/94, Judgement of 28 June 2001.

Von Hannover v. Germany (App no 59320/00) (2004) ECHR 294.

W. v the Netherlands (App no 20689/08), 20 January 2009.

X and Y v the Netherlands judgment of 26 March 1985, Series A no 91.

Y.F. v Turkey (App no 24209/94) ECHR 2003-IX.

Z. v Finland (1998) 25 EHRR 371.

EUROPEAN COMMISSION OF HUMAN RIGHTS

McVeigh, O'Neill and Evans v United Kingdom (1981) 25 DR 15.

List of Legislation

TAIWAN

Constitution of the Republic of China (Taiwan)

Civil Code

Computer-Processed Personal Data Protection Law

Criminal Code

Personal Data Protection Law

Radio and Television Act

Cable Radio and Television Law

Satellite Broadcasting Law

Telecommunications Act

Communications Protection and Surveillance Law

Fundamental Communications Act

Social Order Maintenance Law

THE UNITED KINGDOM

European Community Act 1972

Data Protection Act 1998

Human Rights Act 1998

THE COUNCIL OF EUROPE

European Convention on Human Rights

Convention for the Protection of Human Rights and Dignity of the Human Being with regard to the Application of Biology and Medicine

Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data

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

THE EUROPEAN UNION

Treaty on European Union

Treaty on the Functioning of the European Union (Treaty establishing the European Economic Community)

Charter of Fundamental Rights of the European Union

Treaty of Lisbon

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)

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 (Directive on privacy and electronic communications)

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 (Data Retention Directive)

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

Regulation (EC) No 444/2009 of the European Parliament and of the Council of 28 May 2009 amending Council Regulation (EC) No 2252/2004 on standards for security features and biometrics in passports and travel documents issued by Member States

Commission Recommendation of 12.5.2009 on the implementation of privacy and data protection principles in applications supported by radio-frequency identification.

THE UNITED NATIONS

Universal Declaration of Human Rights (UDHR)

International Covenant on Civil and Political Rights (ICCPR)

International Covenant on Economic, Social and Cultural Rights (ICESCR)

List of Abbreviations

AIDC	Automatic Identification and Data Capture
APEC	Asia-Pacific Economic Cooperation
ASA	Argument from the Sufficiency of Agency
CCTV	Closed-circuit Television
CPDPA	Computer-Processed Personal Data Protection Law (Taiwan)
DPA	Data Protection Act 1998 (UK)
DPAs	Data Protection Authorities
EC	European Community
ECHR	European Convention on Human Rights and Fundamental Freedoms
ECtHR	European Court of Human Rights
EDPS	European Data Protection Supervisor
EEC	European Economic Community
EMF	Electromagnetic Fields
EU	European Union
FMR	False Match Rate
FNMR	False Nonmatch Rate
FTE	Failure-to-enrol Rate
GCA	Generic Conditions of Agency
GPS	Global Positioning System

GSM	Global System for Mobile communications
HRA	Human Rights Act 1998
IAM	Identity and Access Management
ICAO	International Civil Aviation Organisation
ICCPR	International Covenant on Civil and Political Rights
ICERD	International Convention on the Elimination of All Forms of Racial Discrimination
ICESC	International Covenant on Economic Social and Cultural Rights
ICO	Information Commissioner's Office (UK)
ICT	Information, Communication and Technology
ISO	International Organization for Standardization
KMT	Nationalists Party (Taiwan)
LPU	Principle of Universalisability
NFC	Near Field Communication
OECD	Organisation for Economic Cooperation and Development
PETs	Privacy Enhancing Technologies
PGC	Principle of Generic Consistency
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
PNR	Passenger Name Records
PRC	People's Republic of China

RFID	Radio-frequency Identification
SHIP	Scottish Health Informatics Programme
SSRN	Social Science Research Network
TEU	Treaty on European Union
TFEU	Treaty on the Functioning of the European Union
T-PD	Consultative Committee of the 1981 Data Protection Convention
UDHR	Universal Declaration of Human Rights
UK	United Kingdom
USA	United States of America
VIS	European Information System on Visas
WP29	Article 29 Data Protection Working Party

Chapter 1

Introduction

> "And he causeth all, both small and great, rich and poor, free and bond, to receive a mark in their right hand, or in their foreheads: And that no man might buy or sell, save he that had the mark, or the name of the beast, or the number of his name. Here is wisdom. Let him that hath understanding count the number of the beast: for it is the number of a man; and his number is Six hundred threescore and six."
>
> ~13:16-18 Revelation, *The Bible*.

When I came to the UK to study for my PhD, I was required to show my student visa to the (UK) immigration officer. In order to satisfy the border security of the UK, my sensitive personal data had to be collected and processed before I was allowed entry. Although this was the first time that I had visited the UK, this process was not unfamiliar; after all, this is now standard practice in many countries. Ironically, however, the reason why I had come to Britain was to write a thesis exploring what I took to be an experience of having my rights overridden by other interests that are protected by the application of identification and profiling technologies.

1.1 Research Background

The issues that this thesis is concerned with are biometric and radio-frequency identification (RFID) technologies and their routine applications, which enable automated authentication/ verification and identification particularly for purposes of identity managements, e.g., population management, control of entry to both physical and digital areas, and management of health/ research databases.

Advances in identification, tracking and profiling technologies and their expanded applications have never stood still. Indeed, advances in science and technology are frequently claimed to be essential to the general welfare and utility of all in society. It is therefore unsurprising that governments, private enterprises, and individuals claim and apply the right to benefit from those advances. But is there such a right?

This is an important question because it is not surprising that uncontrolled utilisation of the technologies can come into conflict with the protection of fundamental rights and freedoms of individuals.[1] It is almost a statement of the obvious that, even if there is a right to benefit from advanced science and technology, this right can hardly be regarded as an absolute right. When competing rights come into conflict it becomes essential to ascertain how these rights and interests relate to each other, and how to strike a balance between these different values.

It is noted in a report from the European Commission that '[e]thical frameworks for new and emerging fields of science and technology increasingly must address the issue of privacy and data protection issues.'[2] Awareness of these concerns in the

[1] In fact, these concerns may include those other than fundamental rights and freedoms. For example, due to regulatory effectiveness, budget or other political or non-political considerations, there remains a possibility for immigration checks with respect to biometric system to be abandoned on a regular basis. See: BBC, 'Theresa May: Numbers of Unchecked at UK Borders Unknown' *BBC* (London, 7 November 2011) <http://www.bbc.co.uk/news/uk-politics-15615537> accessed 9 November 2011.

[2] René von Schomberg, 'Introduction: Towards Responsible Research and Innovation in the

context of biometrics and RFID has surely compelled advisory authorities as well as academics to look into fundamental rights, in particular privacy and data protection. For example, the independent EU advisory body focusing on data protection issues – the Article 29 Data Protection Working Party (WP29 hereafter)[3] – has adopted a number of specific documents on these two technologies: Working Document on Biometrics,[4] Opinion No 7/2004 on the Inclusion of Biometric Elements in Residence Permits and Visas Taking Account of the Establishment of the European Information System on Visas (VIS),[5] Working Document on Data Protection Issues Related to RFID Technology,[6] Opinion 3/2005 on Implementing the Council Regulation (EC) No 2252/2004 of 13 December 2004 on Standards for Security Features and Biometrics in Passports and Travel Documents Issued by Member State,[7] Opinion N° 3/2007 on the Proposal for a Regulation of the European Parliament and of the Council Amending the Common Consular Instructions on Visas for Diplomatic Missions and Consular Posts in Relation to the Introduction of Biometrics, Including Provisions on the Organisation of the Reception and Processing of Visa Applications (COM(2006)269 final),[8] Opinion 5/2010 on the Industry Proposal for a Privacy and

---

Information and Communication Technologies and Security Technologies Fields' in René von Schomberg (ed), *Towards Responsible Research and Innovation in the Information and Communication Technologies and Security Technologies Fields* (Publications Office of the European Union 2011) 8.

[3] The Article 29 Data Protection Working Party is established by Article 29 of Directive 95/46/EC. Its tasks are laid down in Article 30, Directive 95/46/EC and in Article 15, Directive 2002/58/EC.

[4] Article 29 Data Protection Working Party, *Working Documents on Biometrics* (No 12168/02/EN, WP 80, 2003).

[5] Article 29 Data Protection Working Party, *Opinion No 7/2004 on the Inclusion of Biometric Elements in Residence Permits and Visas Taking Account of the Establishment of the European Information System on Visas (VIS)* (No 11224/04/EN, WP 96, 2004). The main function of the party is to give opinions and advices to the European Commission.

[6] Article 29 Data Protection Working Party, *Working Document on Data Protection Issues Related to RFID Technology* (No 10107/05/EN, WP 105, 2005).

[7] Article 29 Data Protection Working Party, *Opinion 3/2005 on Implementing the Council Regulation (EC) No 2252/2004 of 13 December 2004 on Standards for Security Features and Biometrics in Passports and Travel Documents Issued by Member States* (No 1710/05/EN-rev, WP 112, 2005).

[8] Article 29 Data Protection Working Party, *Opinion N° 3/2007 on the Proposal for a Regulation of the European Parliament and of the Council Amending the Common Consular Instructions on Visas for Diplomatic Missions and Consular Posts in Relation to the Introduction of Biometrics, Including Provisions on the Organisation of the Reception and Processing of Visa Applications (COM(2006)269*

Data Protection Impact Assessment Framework for RFID Applications,[9] Opinion 9/2011 on the Revised Industry Proposal for a Privacy and Data Protection Impact Assessment Framework for RFID Applications,[10] Opinion 2/2012 on Facial Recognition in Online and Mobile Services,[11] and Opinion 3/2012 on Developments in Biometric Technologies.[12]

However, in my opinion, although these attempts have served to raise awareness of the data protection concerns and providing practical guidelines, they have not applied any consistent theoretical framework.[13] This thesis aims to remedy this gap, by developing a framework to assess how to strike a balance between the benefits and the risks of emerging biometric and RFID technologies within a data protection regime.

1.2 Research Questions

---

final) (WP134, 2007).

[9] Article 29 Data Protection Working Party, *Opinion 5/2010 on the Industry Proposal for a Privacy and Data Protection Impact Assessment Framework for RFID Applications* (No 00066/10/EN, WP175, 2010).

[10] Article 29 Data Protection Working Party, *Opinion 9/2011 on the Revised Industry Proposal for a Privacy and Data Protection Impact Assessment Framework for RFID Applications* (No 00327/11/EN, WP180, 2011).

[11] Article 29 Data Protection Working Party, *Opinion 02/2012 on Facial Recognition in Online and Mobile Services* (No 00727/12/EN, WP192, 2012).

[12] Article 29 Data Protection Working Party, *Opinion 3/2012 on Developments in Biometric Technologies* (No 00720/12/EN, WP193, 2012).

[13] For similar attempts in academic field, see, e.g., John D. Woodward and others, *Army Biometric Applications: Identifying and Addressing Sociocultural Concerns* (RAND Publications 2001), Paul de Hert, 'Biometrics: legal Issues and Implications' Background paper for the Institute of Prospective Technological Studies, DG JRC – Sevilla, European Commission <https://public.univie.ac.at/fileadmin/user_upload/inst_staatswissenschaften/Frisch/21063courseWebsite/LegalImplications_Paul_de_Hert.pdf> accessed 9 November 2011, Yue Liu, 'Identifying Legal Concerns in the Biometric Context' (2008) 3: 1 Journal of International Commercial Law and Technology 45-54. Other academic attempts to theorise the issue may fail to offer justifications with regard to the applied theory and clear criterion to deal with the balancing test. E.g., Angela Liberatore, 'Balancing Security and Democracy, and the Role of Expertise: Biometrics Politics in the European Union' (2007) 13 Eur J Crim Policy Res 109-137, Yue Liu, 'The Principle of Proportionality in Biometrics: Cases Studies from Norway' (2009) 25 Computer Law & Security Review 237-250 and Jeremy Wickins, 'The Ethics of Biometrics: the Risk of Social Exclusion from the Widespread Use of Eletronic Identification' (2007) 13 Sci Eng Ethics 45-54, 52.

The central question that the thesis is concerned with and seeks to examine is:

How do we strike a balance between the benefits and the risks of biometric and RFID technologies within a data protection regime, with specific reference to the Taiwanese context?

To answer this question, this thesis will:

1. Identify and justify an adequate theoretical framework to deal with the question;
2. Probe and evaluate current regulation of biometric and RFID technologies in Europe and Taiwan;
3. Provide clear guidelines and principles for legal regulations to deal with the two technologies considered; and
4. Produce a coherently theorised regulatory framework and rule for Formosan[14] data protection law regime.

It should be noted that a handful of core themes will run across most chapters of the thesis. These include discussions of the concepts of privacy, consent, trustworthiness, the balancing of competing rights, and institutional frameworks.

1.3 Methodology

The first task of the thesis is to identify an applicable theoretical framework. This

[14] The Chinese name of 'Taiwan' is also known, especially in the past, as 'Formosa.' This is from Portuguese *Ilha Formosa* as "Beautiful Island," given by the European (Portuguese) explorers in the 16th century. Allan J. Shackleton, *Formosa Calling: An Eyewitness Account of the February 28th 77947 Incident* (The Taiwan Publishing Co. 1998) 1. The formal (English) name of the country is the Republic of China (Taiwan).

thesis employs the moral theory of Alan Gewirth, which requires questions of rights and other normative issues to be referred to within the framework of Gewirth's **Principle of Generic Consistency** (PGC).[15]

I will outline the PGC and its justification and indicate how it can be used to adjudicate relevant potential conflicts. I will then apply the PGC to the European legal regime, evaluate regulation of biometric data at the European level in relation to the PGC, compare the Taiwanese situation to the European one, and suggest a PGC-compliant regulatory framework and rules for Taiwan.

The thesis is conducted primarily through a library-based method, consisting of a literature review from richly diverse sources, including books, journals, official documents, case comments, and websites of both Western (mainly Transatlantic) and Formosan origin.

It is not my intention to describe the laws of Europe (including the ECHR and EU jurisdictions) and then simply compare them to the laws of Taiwan. Instead, the thesis focuses on the issues of privacy, data protection, and the right to benefit from advances of science and technology in general terms to find an applicable framework, and then uses Europe and Taiwan as two substantial case studies to illustrate how the same principles apply in different contexts.

1.4 The Road Map for the Thesis

The thesis consists of nine chapters including this introductory remark as its **Chapter 1**.

[15] Alan Gewirth, *Reason and Morality* (University of Chicago Press 1978).

To arrive at a background understanding of biometric and RFID technologies and to achieve essential clarity for later discussions, in **Chapter 2**, I provide an overview of them and data protection concerns associated with the two technologies.

Although there are a number of social concerns regarding biometrics and RFID, the major concern involves data protection issues. In Chapter 2, two questions concerning biometric data are addressed: (1) whether biometric data is subject to data protection law; and (2) whether biometric data is a type of sensitive personal data. The thesis argues that biometric data should be regarded as sensitive personal data on the basis of a relatively generous interpretation of personal data. With regard to RFID technology, unawareness function creep and concerns of tracking and profiling personal data extend the risks of new technologies. Both of them thus demand a 'smart' regulatory approach[16] and clear guidelines and principles within a data protection regime. To obtain a better understanding of this idea, some real-life examples of specific biometric applications are then provided.

Chapter 3 tackles the fundamental task of answering the research question, which is to provide an adequate theoretical framework. This raises the question of the particular choice and justification of the theoretical approach taken.[17] In this light, I offer reasons for the adoption of the PGC. This includes engaging with critiques of Gewirth's argument for the PGC. Two things must be done here: to outline the PGC and its justification; and to show how the theory can be used to adjudicate relevant

[16] In this regard, Brownsword puts that it is essential for the regulators to be more imaginative and avoid the idea of 'one regulatory size fits all.' See: Roger Brownsword, *Rights, Regulation, and the Technological Revolution* (OUP 2008) 12. Also, citing from above: Neil Gunningham and Peter Grabosky, *Smart Regulation* (Claredon Press 1998) and Ian Ayres and John Braithwaite, *Responsive Regulation* (OUP 1992).

[17] Bernd Carsten Stahl, 'IT for a Better Future. How to Integrate Ethics, Politics and Innovation' in René von Schomberg (ed), *Towards Responsible Research and Innovation in the Information and Communication Technologies and Security Technologies Fields* (Publications Office of the European Union 2011) 25-26.

potential conflicts.

The PGC is a principle governing how agents ought to regard and act towards one another, by requiring that agents act in accordance with the generic rights of all agents. Needs of agency are generic if they are prerequisites of an ability to act at all or with any general chances of success, regardless of the purposes being pursued. Gewirth has argued that 'agents contradict that they are agents if they do not accept that the PGC is the supreme principle governing the permissibility of actions.'[18] The argument is thus an argument produced in the self-reflection of an agent on what is to be an agent. I will contend that major criticisms have been unsuccessful, and I will show how the PGC can justify human rights. But, because this is contentious, I will also argue that anyone who recognises a right to do something must also accept that there is a right to the necessary means and conditions to exercise the mentioned right.[19] Therefore, one cannot sincerely grant human rights without granting rights to the generic conditions of agency protected by the PGC.

Furthermore, I will argue that if the first and least contentious stage of Gewirth's argument for the PGC is valid, then when its conclusion is conjoined with the impartiality assumption contained in the idea that all human beings are equal in dignity and rights, which is a universal value proclaimed by international human rights instruments, then the PGC itself must be accepted.[20] Consequently, even if Gewirth's dialectically necessary argument is unsound, the PGC should be accepted by those who believe that there are human rights as these are currently understood.

---

[18] Gewirth (n 15) 42-47.

[19] Deryck Beyleveld, *The Dialectical Necessity of Morality: An Analysis and Defence of Alan Gewirth's Argument to the Principle of Generic Consistency* (The University of Chicago Press 1991) 15-41. Also, Deryck Beyleveld and Shaun D. Pattinson, 'Moral Interests, Privacy, and Medical Research' in Michael Boylan (ed), *International Public Health Policy and Ethics* (Springer Netherlands 2008) 48.

[20] Deryck Beyleveld, 'The Principle of Generic Consistency as the Supreme Principle of Human Rights' (2012) 13 Human Rights Review 1-18.

This chapter also introduces Gewirth's criterion of degrees of needfulness for action, which states that, in cases of conflict, rights to things that are needed for very possibility take precedence over the rights to things are generically needed to be able to act successfully, without thereby being needed for the vary possibility of acting. The latter rights, in turn, override rights to things that are needed generically to be able to improve one's capacities for successful action. On this basis, the PGC is able to reconcile competing interests and rights.

Building on the Gewirthian framework of a generic condition of agency analysed in Chapter 3, **Chapter 4** seeks to bring the specific application of the PGC more clearly into focus. This is managed in two main steps.

Since the right to privacy is the main (but not the only) fundamental right with which data protection is concerned, the starting point of the chapter is to examine whether and in what way the PGC supports the existence rights that are generally recognised as falling under the heading of a 'right to privacy' in human rights instruments.

The second step switches to the question of how to specifically apply the PGC to the research question. The thesis takes Article 8 of the European Convention on Human Rights (ECHR) as an example. The ECHR does not, however, indicate any explicit guidance on how to strike a balance amongst the rights that it grants. Granted, the ECHR does not accord the PGC official standing. This does not, however, mean that it could not be brought to the European Court of Human Rights (ECtHR).[21] If the arguments for the PGC are valid and the ECtHR can be persuaded of their validity

[21] Deryck Beyleveld and Roger Brownsword, *Human Dignity in Bioethics and Biolaw* (OUP 2001) 76-77. Also, Deryck Beyleveld, 'Data Protection and Genetics: Medical Research and the Public Good' (2007) 18 King's Law Journal 286.

then the PGC could (as it should) be an applicable theory in interpreting the ECHR and dealing with such questions.

The specific application of the PGC will be carried out by identifying the rights granted by Article 8 of the ECHR, valuing the rights in the light of the generic conditions for action, and deciding which of these take precedence. The tension between different conceptions of rights will be vividly brought out by the local cases in the two data protection regimes. In this regard, the added value of the PGC comparing with the ECHR balancing test is fully presented.

Before raising subsequent issues in relation to comments on how the European and Formosan privacy and data protection laws fare in the light of the PGC, it is essential to provide some necessary legal information. **Chapter 5** thus offers an interpretive description of privacy and data protection legislations regarding biometric and RFID technologies in Europe and Taiwan. This starts by reviewing the historical track of European data protection law. Although the primary legislative source of European data protection law is rather complex, it is clear that Directive 95/46/EC (the Data Protection Directive)[22] is the main regulatory instrument in Europe. With this in mind, the chapter reviews the relationship between the Data Protection Directive and other European data protection instruments. This is followed by an overview of data protection law at the UK level. The European part of this chapter ends by looking at the data protection law in relation to biometric and RFID applications.

As regards the Formosan side, Chapter 5 begins the inquiry by critically

[22] 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 [1995] OJ L 281.

surveying Formosan primary statutory privacy and data protection provisions and surrounding constitutional interpretations, followed by a section examining the contents of the right to privacy. After doing so, the last section identifies issues that need to be commented on under the PGC.

In **Chapter 6**, the identified privacy and data protection issues are examined through the lens of the PGC. The preliminary question to be examined is whether there is a right to benefit from advances in science and technology. If so, should it be regarded as a generic right? The thesis argues that there is such a right and, indeed, such a right should be taken into account as a generic right. However, since this right is unsurprisingly not an absolute right, its relationship with other rights must be considered. For the purposes of the thesis, privacy and data protection rights are the ones considered.

I address privacy issues in three main categories, namely spatial privacy, decisional privacy, and informational privacy. Questions such as the level of control over one's body, decisional privacy as 'liberty as licence/ liberty as independence', the 'nothing to hide' argument about informational privacy, and informational privacy and technology, are examined.

In relation to personal data protection provisions, I differentiate the question of (1) conditions under which a right is not engaged from (2) the question of when an engaged right is overridden. I argue that if there is no violation of a generic right (which will be the case when a problematic activity is validly consented to) then there is no need to provide a substantive justification by appeal to an overriding conflicting right.[23] Correlatively, I argue that, when a generic interest is engaged, in the absence

[23] Deryck Beyleveld and Roger Brownsword, *Consent in the Law* (Hart Publishing 2007) 238.

of consent, wrongs can only be justified by a PGC-sensitive substantive justification.[24] In light of this, after undertaking the groundwork in relation to consent, I move on to identify and comment on the problem of integrity of consent in Article 6 of the Personal Data Protection Law (PDPL). This is followed by a discussion focusing on the substantive justification with respect to a specific justification in Article 6 of the PDPL, namely the right to academic research. However, it should be borne in mind that different values and interests do not necessarily come into conflict. This invites the introduction of 'the co-operation model.'

In **Chapter 7**, adequate principles and guidelines to safeguard privacy and data protection when dealing with technologies are proposed. Instead of 'a conflict model' which is coupled with a narrow conception of privacy, this chapter adopts 'the co-operative model' suggested by Beyleveld.[25] The 'co-operative model' employs a broad conception of privacy under which it is possible to view potentially conflicting values as supporting each other. By focussing on this possibility, it facilitates a positive-sum outlook which is more likely to enable the rights at issue to be given the weight they merit.

It has been argued that the justification of the acceptance of a broad concept of privacy can justify the co-operative model.[26] Three types of justification are provided in this respect, namely the legal, ethical and pragmatic reasons. With this in mind, this chapter demonstrates two key privacy and data protection enhancing mechanisms, which demonstrate the practicability of the co-operative model, namely Privacy Impact Assessment (PIA) and Privacy Enhancing Technologies (PETs). It then moves

[24] Ibid 238.
[25] See Deryck Beyleveld, 'Conceptualising Privacy in Relation to Medical Research Values' in Sheila AM McLean (ed), *First Do No Harm: Law, Ethics and Healthcare* (Ashgate Publishing 2006) 156-158. Also, Beyleveld, 'Data Protection and Genetics: Medical Research and the Public Good' 275-289.
[26] Beyleveld, 'Conceptualising Privacy in Relation to Medical Research Values' 158.

on to addressing the operationalisation of the co-operative model. In this regard, I argue that the creation and maintenance of trust between those with possible conflicting interests must be the focus in designing a general regulatory position on the basis of the co-operative model. In applying these frameworks, I suggest that a well-designed framework can improve trustworthiness between data subjects and data controllers. At the end of the chapter, it is contended that legal regimes should be in favour of an independent authority regulatory designed to facilitate dealing with privacy and data protection issues regarding technologies.

Building upon the previous discussion, **Chapter 8** attempts to tie the threads of this work together and to offer a PGC-compliant regulatory framework and rule for Taiwan. At the beginning of this chapter, I critically survey the analytic comparison of regulatory positions between the European and Taiwanese situations of the two technologies. It is observed that the objectives and principles of data protection are similar in both areas, as the Formosan data protection law regime borrowed a number of experiences from the influential European data protection model. However, as held in J. Y. Interpretation No. 603: '[d]espite the admissibility of other nations' similar legislations [sic] and domestic popular polls as materials used in interpreting the Constitution, they cannot be used as the sole basis of determining the meanings and intents thereof.' In response, three differences between the two regimes are considered; differences of handling consent versus public interests; differences in giving effect to data protection principles; and differences concerning the existence or absence of supervisory authorities. The main issue considers which positions are compatible with the requirements of the PGC, taking into account different regulatory methods.

Based on the understanding of this analysis, this chapter then proposes a PGC-derived regulatory framework and rule for Taiwan. Recommendations in

applying the co-operative model to legislations and the institutional framework are made in this regard.

Conclusions are drawn in **Chapter 9**.

By relating the PGC to European and Taiwanese privacy and data protection legal regimes, it will have been argued that Gewirth's moral theory is able to assist, in theory and in practice, with striking a balance between the benefits and the risks of biometric and RFID technologies. To be clear, however, it is also submitted that defending the Gewirthian moral theory is by no means the main task of this thesis.[27] Rather, espousing the PGC and the criterion of degrees of needfulness for action, enables us to identify which rights are covered and to compare the competing rights and interests (and decide which rights can override other rights).

Moreover, the co-operative model, based on the Gewirthian thinking, suggests that competing values may not always belong to two mutually exclusive sets. A corollary of this work, in particular Chapters 7 and 8, is meant to provide guidance on the way to enhance and operationalise the model to deal with benefits and concerns of science and technology as well as their applications. It is noted that, however, this thesis does not intend to provide recommendations in effect to guide the European and Formosan data protection law regimes and ethical codes with respect to the two technologies. Instead, the purpose of this thesis is, again, to make the case for the PGC, as a theoretical framework, to be further applied in the future in order to avoid the emergence of 'policing countries.'[28] With this in mind, while I have no doubt that

[27] For the defending of the PGC, see, e.g., Deryck Beyleveld and Roger Brownsword, *Law as a Moral Judgement* (Sweet and Maxwell 1986), Beyleveld, *The Dialectical Necessity of Morality: An Analysis and Defence of Alan Gewirth's Argument to the Principle of Generic Consistency*, and Beyleveld, 'The Principle of Generic Consistency as the Supreme Principle of Human Rights' 1-18.

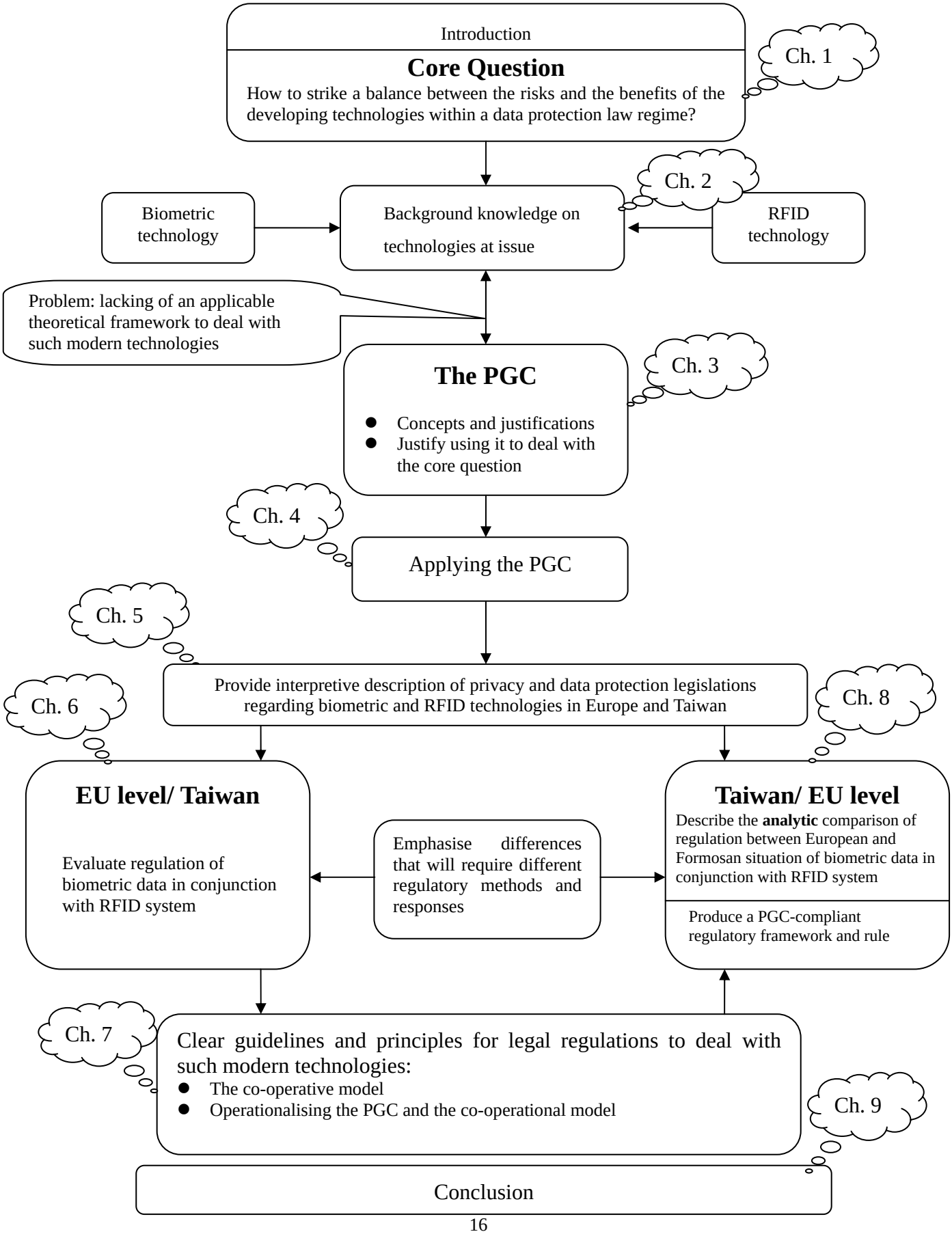
[28] It has been argued that 'there is a further trend towards a reduction in the functional separation between public entities, and a change in the boundaries between the public and the private sectors' by a

governance in both data protection regimes is suboptimal and thus can be improved upon, I believe that lessons for Taiwan may be learned from the European data protection experience and vice versa.

The structure of the thesis can be briefly expressed in the following map:

report produced by Foundation for Information Policy Research. In this report, it has also been argued that this may drive the risk of policing country. See Foundation for Information Policy Research, *Paper No. 5: Conclusions & Policy Implications* (UK Information Commissioner Study Project: Privacy & Law Enforcement, 2004). Available at: <http://www.ico.gov.uk/upload/documents/library/corporate/research_and_reports/conclusion_and_policy_options.pdf> accessed 19 October 2009.

The Map of the Thesis



Chapter 2

Modern Technologies and Data Protection Law:

Setting the Scene

2.1 Introduction

It will not be surprising if lawyers are unfamiliar with the technical terms used in the field of (bio)technology and the law. To assist with this, this chapter will provide an overview on biometric and RFID technologies as a point of departure for later exploration. The extensive international literature on data protection issues regarding biometrics and RFID, particularly from a European perspective, will be examined here.

The chapter is divided into three sub-sections: (1) biometric technology; (2) RFID technology; and (3) data protection concerns associated with these technologies. After providing definitions and introducing new technologies, it will then assess both benefits and risks of these new technologies. On the one hand, certain technologies promise benefits such as introducing a safer and more convenient future. On the other hand, they can also pose risks, or at least raise concerns about their safety and convenience.[1] Consequently, regulating these new technologies requires a persuasive and suitable framework that is able to strike a balance between the benefits and the risks. Before presenting such a framework, real examples of the regulation of these

[1] It should be noted that this thesis concentrates on legal perspective rather than the field of science & technology studies (STS).

technologies will be provided.

2.2 Biometrics and Its Applications

2.2.1 Key Terms and Its Process

Numerous definitions of biometrics exist. In the words of Wei and Li 'biometrics is statistical study of biological data' and 'the science of measuring and statistically analysing biological data.'[2] The Article 29 Data Protection Working Party (WP29) states that 'biometric systems are applications of biometric technologies, which allow the automatic identification, and/or authentication/verification of a person.'[3] In its report: *Army Biometric Applications: Identifying and Addressing Sociocultural Concerns*, the RAND institution suggests that biometrics is 'any *measurable, robust, distinctive, physical characteristic* or *personal trait* of an individual that can be used to *identify or verify* the claimed identity of, that individual.'[4] The recent proposal for an EU General Data Protection Regulation, specifies in Article 4(11) that biometric data 'means any data relating to the physical, physiological or behavioural characteristics of an individual which allow their unique identification, such as facial images, or dactyloscopic data.'[5]

---

[2] Gang Wei and Dongge Li, 'Biometrics: Applications, Challenges and the Future' in Katherine J. Strandburg and Daniela Stan Raicu (eds), *Privacy and Technologies of Identity: A Cross-disciplinary Conversation* (Springer 2006) 136.

[3] Article 29 Data Protection Working Party, *Working Documents on Biometrics* (No 12168/02/EN, WP 80, 2003) 3.

[4] John D. Woodward and others, *Army Biometric Applications: Identifying and Addressing Sociocultural Concerns* (RAND Publications 2001) 9. Available at: <http://www.rand.org/pubs/monograph_reports/MR1237/> accessed 4 November, 2009.

[5] European Commission, '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)' (2012) <http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf> accessed 30 Janurary 2012.

For the purposes of the thesis, 'characteristics', 'utilities', 'presentations', and 'applications of biometrics' need some further explanation.

First, as far as the technical terminology of biometrics is concerned, there are some essential elements[6] regarding the evaluation of whether a specific characteristic is suitable for biometric applications, namely:

- Automaticity: a biometric system is automatically performed and processed by computers or digital machine networks instead of manually by a human. In other words, it is electronic equipment, not human beings[7] that measure and statistically analyse biological personal data.
- Measurability: biological traits or data have to be measurable in order to be saved into the system in a digital form and presented to a sensor based on accuracy and speed of recognition of measurement regarding the operational and environmental factors involved. This includes characteristics of *universality*,[8] *collectability, performance* and *acceptability*.
- Distinctiveness (Uniqueness): biological personal data need to be unique in order to serve their purpose of *identifying/ verifying* the claimed identity of a

[6] It has been observed that there are seven pillars of biometrics: (1) universality, (2) distinctiveness, (3) permanence, (4) collectability, (5) performance, (6) acceptability and (7) resistance to circumvention. See: Anil Jain, Ruud Bolle and Sharath Pankanti, 'Introduction to Biometrics' in Anil Jain, Ruud Bolle and Sharath Pankanti (eds), *Biometrics: Personal Identification in Networked Society* (Kluwer Academic Publishers 1999) 1-42. Also, European Commission Joint Research Centre, Institute for Prospective Technology Studies 'Biometrics at the Frontiers: Assessing the Impact on Society' (2005) 37. Available at:
< http://ec.europa.eu/justice_home/doc_centre/freetravel/doc/biometrics_eur21585_en.pdf> accessed 20 November, 2009. The Irish Council for Biometrics, *Biometrics: Enhancing Security or Invading Privacy? Opinion* (The Irish Council for Biometrics 2009) 2-3. Available at:
< http://www.bioethics.ie/uploads/docs/Final_Biometrics_Doc_HighRes.pdf> accessed 20 November, 2009.

[7] In fact, both physical and behavioural biological characters are regularly used to 'manually' verify or check identity. For example, imagine you see your colleague's face, which is a sort of physical characteristic, and you recognise him and then greet him; or, you sign your name, which is a behaviour biological characteristic, when using a credit card and the cashier compares it with your signature which is shown on your card. See also: Samir Nanavati, Michael Thieme and Raj Nanavati, *Biometrics: Identity Verification in a Networked World – A Wiley Tech Brief* (John Wiley & Sons, Inc. 2002) 9.

[8] The WP29 addressed this feature as 'universal', which indicates that 'the biometric element exists in all persons'. *Article 29 Data Protection Working Party*, (n 3) 3.

given person. The degree of uniqueness determines the application kind of a biometric system. For instance, a low degree of uniqueness occurs when identical twins are facially-scanned; so, this may not be an ideal application of such a biometric system. In order to measure the data accurately, means to secure the difficulty are required to defeat or bypass the biometric system. This additionally shows the feature of *resistance to circumvention*.

- Permanence: if a key can be changed or damaged easily, then it is not ideally designed to serve its purpose. As the RAND report explains: '[t]he robustness of a biometric is a measure of the extent to which the physical characteristic or personal trait is subject to significant change over time.'[9] The degree of stability over time, also, determines the application of biometric system. For example, there may be a greater chance for the voice-scan system of incorrectly judging a teenager during her/ his period of puberty because of the voice change.

Secondly, as regards the utility of biometric technology, this is either for *verification* or *identification*. The former involves a so called one-to-one (1:1) search.[10] It implies checking the identity claim showed by a user to the system for a biometric comparison which could be referred as answering the 'Am I who I *claim to be?*' question.[11] On the other hand, the identification model, also known as recognition,[12] involves a one-to-many (1:N) search as one piece of individual data being compared against many recorded data. The user needs to provide her biometric data in advance, and then the system matches this data with a (normally large) number

[9] Woodward and others (n 4) 10.
[10] Ibid 12-13. Also, Ishwar K Sethi, 'Biometrics: Overview and Applications' in Katherine J. Strandburg and Daniela Stan Raicu (eds), *Privacy and Technologies of Identity: A Cross-disciplinary Conversation* (Springer 2006) 118.
[11] Nanavati, Thieme and Nanavati (n 7) 12.
[12] Sethi (n 10) 118.

of users to identify the person. It answers the question of 'Who *am I?*'[13]

Thirdly, in connection to the description of this technology, it is based on unique measurements of physiological or behavioural characteristics, or sometimes the combination of both.[14] The physiological form at least contains data types such as fingerprints, face recognition, DNA, hand and palm geometry, iris recognition and retina recognition. Examples of the latter, on the other hand, include voice, signatures, keystroke dynamics and gait analysis. Applications of different biometric associated technologies such as finger-scan, facial-scan, voice-scan, iris-scan, signature-scan, hand-scan, retina-scan, keystroke-scan,[15] and DNA-scan[16] technologies, can either be done individually or in combination. It is noted that the above examples cannot be seen as an exhaustive list for biometric types as new techniques keep developing rapidly. Moreover, due to different specific purposes of the application, it is impossible to identify which type of biometrics is the 'best' one to apply.[17]

The presentation of a system has four stages:[18] sensor or data capture, pre-processing, feature extraction, and recognition. The last stage could be carried out in one of two possible ways: *classification* or *matching*. The former method simply uses one or more mathematical functions. The latter is 'performed by comparing the extracted properties of the input pattern against the set of stored properties representing different patterns that the system is capable of recognising.'[19] Here, 'the

---

[13] Nanavati, Thieme and Nanavati (n 7) 12-13.
[14] For further knowledge in relation to leading physiological or behavioural biometric modalities, see: ibid 43-140. Also, The Irish Council for Biometrics (n 6) 18-58.
[15] For further knowledge in relation to leading physiological or behavioural biometric technologies, see: Nanavati, Thieme and Nanavati (n 7) 43-140.
[16] The Irish Council for Biometrics (n 6) 50-54.
[17] James L. Wayman and others, 'An Introduction to Biometric Authentication Systems' in James L. Wayman and others (eds), *Biometric Systems: Technology, Design and Performance Evaluation* (Springer 2005) 3-4.
[18] Sethi (n 10) 119, citing Richard O. Duda and Peter E. Hart, *Classification and Scene Analysis* (John Wiley & Sons, Inc. 1973).
[19] Sethi (n 10) 120.

set of stored properties' is also known as the *template.*[20]

2.2.2 The Promised Benefits

Generally, biometric technologies promise two main benefits: *security* and *convenience*. This can be observed by comparing the other two traditional authentication methods: knowledge based and token based ones.[21] The former depends on the knowledge that a genuine system user should have, for example, the password or the personal identification number (PIN). The latter relies on presenting legitimate tokens given by system controllers. Different from the questions such as '*Are you who you claim to be?*' and '*Who are you?*' asked by biometric technology, these two traditional authentication methods inquire '*What do you know?*' and '*What do you have*?' It is easy to find daily applications combining these two methods. For instance, a debit card (which is a token) is only usable after the user inputs her PIN.

The main shortcoming of traditional authentications is that they may be guessed, lost or stolen easily. This is because those tokens/PINs are not tightly coupled with their owner's identity.[22] Knowledge-based methods, for example, could fail because the user forgets her password, which may be complex or unfamiliar to her. Possible solutions to this problem are either to write down the password on an unprotected medium such as a single piece of paper stored in her wallet, or to have a simpler password to memorise – which is always associated with her (such as her birthday,

[20] According to Samir Nanavati et al., a template 'is a small file derived from the distinctive features of a user's biometric data, used to perform biometric matches.' For further knowledge about the template, see: Nanavati, Thieme and Nanavati (n 7) 18-19.
[21] L. O'Gorman, 'Comparing Passwords, Tokens, and Biometrics for User Authentication' (2003) 91 Proceedings of the IEEE 2021-2040.
[22] Alisher Kholmatov, *Privacy Protecting Biometric Authentication Systems – A Novel Framework to Protect Privacy* (VDM Verlag 2009) 2.

address, or telephone numbers). However, it is not difficult to imagine that this knowledge may get lost or stolen, and an attacker could get access to all the other applications used by the same user – if her passwords are all the same or similar.

On the other hand, the tokens for token based authentication approaches nowadays are usually rather tiny and easy to carry – which, however, means that there are increased risks of them getting lost or stolen. Moreover, because the user needs to memorise the key or carry the token items, which may be difficult for older or disadvantaged people, traditional authentication approaches are not convenient/ safe enough for specific groups of individuals. Overall, there are higher chances for these traditional 'token-based keys' or 'knowledge-based passwords/pins' to be used in an unauthorised manner.

Biometrics, however, could solve this problem. The features of biometrics – automaticity, measurability, uniqueness and stability over time – provide benefits on both *safety* (biometric traits are harder to imitate or share) and *convenience* (there is no need to carry or remember anything) which are tightly coupled with identity of users. Etzioni, therefore, contends that '[i]f individuals could be properly identified, public safety would be significantly enhanced and economic costs would be reduced significantly.'[23]

2.2.3 The Potential Risks

Nothing is perfect. Alongside the described benefits, biometric techniques carry some potential risks. The two main types of risks are (1) technical problems, and (2) social

[23] Amitai Etzioni, *The Limits of Privacy* (Basic Books 1999) 104.

concerns.

The first problem arises from the imperfect nature of biometric techniques: 'false rates' will never (or at least hardly ever) be zero.[24] To explain briefly, 'false rates' may exist as 'false accept' errors or 'false reject' errors in three ways. Firstly, *false match rate* (FMR) means the probability that a biometric system user's template 'will be incorrectly judged to be a match for a different user's template.'[25] Secondly, *false nonmatch rate* (FNMR) indicates 'the probability that a user's template will be wrongly judged to *not* match her/his enrolment template.'[26] Generally speaking, the higher the degree of susceptibility to changes in biometric data, user presentation, and environment of the live-factors of these application technologies, the lower FNMR will be. Thirdly, *failure-to-enrol rate* (FTE) indicates 'the probability that a given user will be unable to enrol in a biometric system.'[27]

High threshold biometric technologies such as iris-scan or retina-scan result in higher FNMR or FTE due to susceptible changes. On the other hand, low threshold ones such as face-scan or signature-scan have higher FMR based on its level of accuracy. It is fair to say that, therefore, there is no perfect biometric technology (at least to date) because there is never a conclusive match.

Though it seems to be safer and more convenient than other traditional authentication methods, it is, actually, *not* as safe and convenient as it is generally assumed. The statistics demonstrate that popular forms of fingerprint, face and voice biometrics all have their error rates (including FMR and FNMR) exceeding the 0.1

[24] Article 29 Data Protection Working Party, *Opinion 3/2012 on Developments in Biometric Technologies* (No 00720/12/EN, WP193, 2012) 6.
[25] Nanavati, Thieme and Nanavati (n 7) 24-27.
[26] Ibid 27-33.
[27] Ibid 33-38.

percent level.[28] Furthermore, it is, in fact, *not too difficult* to deceive most of the popular biometric systems/ applications. For instance, an easy-to-make rubber copy of a person's fingerprints can effortlessly trick the system.[29] In addition, a study concluded that '[a]ll tested fingerprint readers were defeated with artificial fingerprints.'[30] Biometric data theft, in this respect, could even have worse consequences in comparison with traditional methods. This is because the biometric data of the user cannot be easily changed or re-issued. Therefore, there is a potential danger of relying on these technologies as the *only* and *definite* authentication methods.

Moreover, the two major advantages of biometrics, namely safety and convenience, may conflict – safer (more unique) forms of biometric traits are less convenient because the rate of acceptance of the system is lower. Unique forms of biometric trait reducing FMR are harder to forge. Yet they cause higher FNMR and FTE. Therefore, if the user is not accepted, she may need to provide alternative evidence of her identity or she will be rejected by the system. The problem here is that the user may not be able to access the needed systems, though she is exactly who she claims to be.

Additionally, although the cost of biometric applications has been considerably reduced, financial issues in relation to the applied facilities may still occur. For

---

[28] Anil K. Jain and Sharath Pankanti, *Beyond Fingerprinting: Is Biometrics the Best Bet for Fighting Identity Theft?* (Scientific America Magazine 2008). Available at: <http://www.scientificamerican.com/article.cfm?id=beyond-fingerprinting> accessed 18 November 2009.

[29] Tsutomu Matsumoto, 'Importance of Open Discussion on Adversarial Analyses for Mobile Security Technologies, International Telecommunication Union' (Telecommunication Standardization Sector, International Telecommunication Union Workshop on Security).

[30] Drew Robb, *Authentication with a Personal Touch: Fingerprint Scanners Are Accurate Biometric Identification Tools - But They're Not Foolproof* (Government Computer News, 2005 WLNR 26140142, 2005), cited from Daniel J. Solove, *Nothing to Hide: the False Tradeoff between Privacy and Security* (Yale University Press 2011) 202.

example, the budget burden of biometric ID cards, with higher costs for using more unique forms of biometric systems, or systems that combine two or more kinds of biometric data, can be a controversial issue after a cost-benefit analysis is conducted. Example could be found in the UK ID cards policy debate regarding its high cost budgets.[31]

Secondly, a number of social concerns can stem from applying biometric systems. For example, the RAND Institute's report identifies three key 'sociocultural concerns': physical issues, religious objections, and informational privacy.[32] It lists physical concerns including stigmatisation, actual harm (for example, those people whose careers depend on their eyesight may be worried about iris or retina scans), and hygiene issues (one may feel uncomfortable about placing one's body parts against a machine; this problem, however, could be solved by using RFID technology which is a wireless one).[33] In terms of religious objections, certain Christians, for example, on the basis of the language in Revelation (shown in the introductory remark of this thesis),[34] may regard biometric technologies as the application of 'Beast Marks' in the modern age.

Moreover, social concerns also arise from applying biotechnologies to a national/ international-wide scope database. This is because such identification and database may be a tool for 'greater government surveillance and can be used to track people's movement.'[35] Indeed, fears of the metaphor of Big Brother in relation to data

[31] The Department of Information Systems, LSE, *The Identity Project: An assessment of the UK Identity Cards Bill and its implications* (version 1.09, LSE, London 2005) at: <http://is2.lse.ac.uk/IDcard/identityreport.pdf> accessed 18 November 2009.
[32] Woodward and others (n 4) 21-31.
[33] Ibid 26-27.
[34] Ibid 28.
[35] Solove (n 30) 201.

profiling, e.g., the fear of Orwellian,[36] have been called into question.[37] It has been argued that, relying on the historical precedents of World War II and post-war periods, and a general fear about tracking citizens through operated filing systems, past experiences have influenced 'the development of philosophical notions of inalienable rights of the individual' in Europe.[38] In this regard, without proper democratic processes such as adequate representatives and public hearings, worries in relation to transparency and legitimacy may occur.[39] With respect to such a large-scale biometric database, furthermore, issues concerning discrimination should be noted. It is observed that, for example, applying biometric technologies *in general* is unfair to disabled or disadvantaged people, as they could not, practically, provide specific form of biometric traits/ samples or simply these technologies do not allow for sufficient distinguishing characteristics.

Last but not least, providing biometric traits/ samples and data may contain other kinds of *sensitive data*.[40] For example, McLean's study showed that palm skin, which is needed for a hand-scan, may reveal certain genetic disorders.[41] Fingerprints,

---

[36] Orwellian indicates the situation of the totalitarianism that the government constantly monitors the individuals to detect betrayal or any unwanted behaviours via "improper" thoughts. This is famously from the literary work *1984* of George Orwell. See, e.g., Simson Garfinkel, *Database Nation : The Death of Privacy in the 21st Century* (O'Reilly Media 2001).

[37] However, Solove argues that it is a wrong metaphor regarding informational privacy and considers that the problem is better captured by the Kafka metaphor (which stems from Franz Kafka's *The Trial*). This is because, as he argues, the problem lies on the 'powerlessness, vulnerability, and dehumanization created by the assembly of dossiers of personal information where individuals lack any meaningful form of participation in the collection and use of their information.' Daniel J. Solove, 'Privacy and Power: Computer Databases and Metaphors for Information Privacy' (2001) 53 Stanford Law Review 1393-1462.

[38] Marek Rejman-Greene, 'Privacy Issues in the Application of Biometrics: a European Perspective' in James L. Wayman and others (eds), *Biometric Systems: Technology, Design and Performance Evaluation* (Springer 2005) 336.

[39] Helen Busby, Tamara K. Hervey and Alison Mohr, 'Ethical EU Law? The Influence of the European Group on Ethics' (2008) 33 Science and New Technologies 804-805.

[40] Kholmatov 6. Also, Gerrit Hornung, 'The European Regulation on Biometric Passports: Legislative Procedures, Political Interactions, Legal Framework and Technical Safeguards' SCRIPT-ed <http://www.law.ed.ac.uk/ahrc/SCRIPT-ed/vol4-3/hornung.asp> accessed 18 November 2009.

[41] W. H. I. Mclean, 'Genetic Disorder of Palm Skin and Nail' (1997) 202 Journal of Anatomy 133-141.

according to Chen,[42] Schuster,[43] and Woodward et al.,[44] may disclose some disease and health data including leukaemia, breast cancer, Rubella syndromes, Down's syndromes, Turner syndromes, and Klinefelter syndromes. Iris and retina biometrics, mentioned by contributions of Woodward et al.[45] and Bates[46] respectively, could be linked with common diseases including diabetes, arteriosclerosis and hypertension. In addition to the above health information, biometric data may even reveal the user's sex life – homosexuality,[47] which is also under the special categories of personal data defined by the Data Protection Directive.[48]

2.3 Radio-frequency Identification (RFID) Technology

2.3.1 Key Terms and Its Process

The following definition[49] of RFID is provided by Commission of the European

---

[42] H. Chen, *Medical Genetic Handbooks* (MO: W.H. Green 1998).

[43] M. M. Schuster, 'Gastroenterology: Fingerprinting gi disease' (1996) April Johns Hopkins Physician Update 5.

[44] John D. Woodward, Nicholas M. Orlans and Peter T. Higgins, *Biometrics: Identity Assurance in the Information Age* (McGraw-Hill 2003) 202.

[45] Ibid 203.

[46] Barbara Bates, *A Guide to Physical Examination and History Taking* (5th edn, Lippincott Williams and Wilkins 1991) 181-215.

[47] J. A. Y. Hall and D. Kimura, 'Dermatoglyphic Asymmetry and Sexual Orientation in Men' (1994) 108 Behavioral Neuroscience 1203-1206. The term of 'dermatoglyphics', according to this report, means 'the characteristics of the ridged skin on the fingertips, palms, toes, and soles of primates and some other mammals.' In this report, the authors remark that '[a]lthough this effect was not accounted for by differences in hand preference, an association was observed between leftward dermatoglyphic asymmetry and an increased incidence of adextrality in homosexual men, but not in heterosexual men.' Available at: < http://www.sfu.ca/~dkimura/Publications/Hall%20&%20Kimura%20(1994).%20Dermatoglyphic%20asymmetry%20and%20sexual%20orientation%20in%20men.pdf> accessed 18 November 2009.

[48] Article 8(1) of Directive 95/46/EC: 'Member States shall prohibit the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life.'

[49] Similar definition is suggested by the RFID Journal. According to the RFID Journal, technically speaking, RFID is used to indicate a system that: (1) transmits the identity, (2) in the form of a unique serial number, (3) of an object or person (who has an RFID tag attached) wirelessly, (4) using radio waves. Available at: < http://www.rfidjournal.com/article/articleview/1339/1/129/> accessed 18 November 2009.

Communities as:

> …the use of electromagnetic radiating waves or reactive field coupling in the radio frequency portion of the spectrum to communicate to or from a *tag* through a variety of modulation and encoding schemes to uniquely *read* the identity of a radio frequency *tag* or other data stored on it. (emphasis added)[50]

Under this definition, there are two main components of RFID: a *tag* that contains an identification number or other stored data, and a *reader* which contains 'electromagnetic radiating waves or reactive field coupling in the radio frequency portion of the spectrum' that works as a scanner. A 'RFID tag' is specified by the EU RFID recommendation as

> …either a RFID device having the ability to produce a radio signal or a RFID device which re-couples, back-scatters or reflects (depending on the type of device) and modulates a carrier signal received from a reader or writer.[51]

RFID tags may have a range of different types. For example, they can be either *active* or *passive*, either *read-only* or *read-write*,[52] and either *wearable* or *implantable*.[53] An 'RFID reader', on the other hand, is

> …a fixed or mobile data capture and identification device using a radio frequency

[50] Section 3(a) of the EU common recommendation of 12.5.2009 on the implementation of privacy and data protection principles in applications supported by radio-frequency identification, SEC(2009) 585 (here after: 'EU RFID recommendation').
[51] Ibid, section 3(b).
[52] Active (battery-powered) tags which contain batteries could broadcast without a RFID reader while passive ones cannot do so due to they depend on power supply from a RFID reader. Read-write tags could update information they carried. Parliamentary Office of Science and Technology, 'Radio Frequency Identification (RFID)' (*Parliamentary Office of Science and Technology*, 2004) <http://www.parliament.uk/documents/upload/POSTpn225.pdf> accessed 18 November 2009.
[53] For example, the wOzNet is kind of wearable tracking device and the VeriChip is an implantable one. See: Paul M. Schwartz, 'Privacy Inalienability and Personal Data Chips' in Katherine J. Strandburg and Daniela Stan Raicu (eds), *Privacy and technologies of identity: a cross-disciplinary conversation* (Springer 2006) 93-113.

> electromagnetic wave or reactive field coupling to stimulate and effect a modulated data response from a tag or group of tags.[54]

Apart from these two infrastructures, the European Data Protection Supervisor (EDPS) suggests that when assessing data protection and privacy issues on RFID technology, 'the network, the reference database and the database where the data produced by the association tag/reader are stored'[55] must be considered at the same time. These key components make RFID tags not simply 'electric tags', but an 'internet of things'[56] because they extend utility to each part of an overall network. The 'internet of things' characteristic relates to the possibility of linking databases and certain communication networks, such as the internet, Global System for Mobile communications (GSM, originally from Groupe Spécial Mobile), Global Positioning System (GPS), and Closed-circuit Television (CCTV) networks. Moreover, building upon RFID, the Near Field Communication (NFC) standard for smartphone devices allows two-way communication between endpoints/ peers, in which traditional RFID devices were one-way communicating only.[57]

For the purposes of the thesis, two important characteristics of RFID should be noted: (1) the *wireless* nature of RFID could enable the remote processing of data that the public is unlikely to be aware of; and (2) a reader could *track* locations of RFID tags on an object or those implanted in human bodies.

---

[54] EU RFID recommandation, section 3(c).

[55] The European Data Protection Supervisor, *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, OJ 2008/C 101/01, 2007) para. 21.

[56] Commission of the European Communities, *Communication form the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Radio Frequency Identification (RFID) in Europe: steps towards a policy framework* (COM (2007) 96 final, 2007).

[57] NFC Forum, 'About NFC' (*NFC Forum*, 2012) <http://www.nfc-forum.org/aboutnfc/> accessed 10 July 2012.

2.3.2 The Promised Benefits

Again, the benefits of the RFID technology can be understood by comparing them to traditional methods. There are three main forms of Automatic Identification and Data Capture (AIDC) technologies: (1) an optical type, such as bar codes, (2) a magnetic type, such as magnetic stripe cards, and (3) an electronic type, such as RFID tags and SIM cards.[58] As with biometrics, the widespread use and rapid adoption of the RFID technology is due to their convenience and security.

First, the reader receives information automatically and wirelessly from the tags, thus enabling the products/people to save time and avoid the disturbance and inconvenience of handing their ID certifications in either optical or magnetic form. Information technologies also have the potential to enable sharing, comparisons, and analyses (profiling) between databases, so that within a set of systems, several services could be run together, which would also reduce costs. Furthermore, tags could store more information than the other two types of AIDC technologies.

Secondly, the ability to trace the location of the tags could improve the safety of products or services such as food, medicines and health care services. It is also harder to copy RFID tags than the other two traditional types of AIDC technologies, which could improve the safety requirements. Consequently, in the context of the modern information society, it seems certain that RFID technology reflects whatever technology could deliver better results for the entire population.

[58] Commission of the European Communities (n 56).

2.3.3 The Potential Risks

Yet, there is no denying that risks related to the widespread application of RFID in the information era need to be fully recognised. Predicaments regarding RFID technology can also be identified in two respects: technical problems and social concerns.[59]

Firstly, there are some technique limitations to RFID and its applications. For instance, the lack of a universal standard of RFID tags, which may restrict its applications at a global-use level, as a result, will increase its *cost* – both on the aspects of installing and of integrating RFID systems into existing setups.[60] Similar problems with regard to inconsistent global standard stem from the assignment of frequencies and power for operation.[61] Therefore, the need to monitor demand may increase with the use of RFID.[62]

Concerns may also arise from an environmental perspective, because of the huge amount of waste produced by electrical and electronic equipment and RFID tags.[63] Furthermore, from a health angle, notwithstanding that RFID applications are generally low in power (active tags may operate with higher power) under normal operating conditions, possible detrimental health effects of exposure to Electromagnetic Fields (EMF) are still to be expected.[64]

The most significant technical problem is, perhaps, the *safety* of RFID. According

---

[59] Some other risks ,which lead to privacy and data protection concerns, such as function creep problem due to the 'internet things' characteristic of RFID, will be discussed in the later part.
[60] Parliamentary Office of Science and Technology (n 52) 2.
[61] Generally speaking, states have the regulatory power for this kind of 'spectrum allocation', as a result, it is unavoidable to drive to an international variation in the for RFID systems. See: Ibid.
[62] For example, EU Commission Decision 2006/804/EC of 23 November 2006 on harmonisation of the radio spectrum for radio frequency identification (RFID) devices operating in the ultra high frequency (UHF) band. See Commission of the European Communities (n 56) 7.
[63] EU regulates those concerns with Directives 2002/96/EC on waste electrical and electronic equipment (WEEE) and 2002/95/EC on the restriction of the use of certain hazardous substances in electrical and electronic equipment (RoHS). See ibid 8.
[64] Ibid 8.

to the Information Commissioner's Office (ICO, UK), a practical problem is known as the 'skimming' of RFID, which presents the possibility of unauthorised access for the sake of picking up signals from tags through any compatible reader.[65] In this regard, information stored in the tags may be 'stolen', or more accurately, be 'cloned' or 'copied.'[66] This may not only result in privacy or data protection concerns, but also in some other criminal offences.[67] Therefore, the ICO recommends that tags with sensitive personal data should be at a higher and adequate level of encryption to prevent this sort of risk.[68]

Secondly, social concerns regarding public databases at a national/ international mass scale may also occur with RFID. For example, customers may have a choice not to apply RFID in private business sectors (whether on the opt-in or the opt-out model); while in the public sphere, citizens may have less choice – such as some ID cards or passports with RFID tags on them. In this respect, it is the controller (the government) of the RFID system who has more power to decide than the users (citizens).[69]

There are, undoubtedly, some unique social concerns raised by RFID. For example, the tracking ability offered by RFID, which opens up the possibility of physically remote tracking by virtue of profiling through undetected surveillance.[70] Another problem stems from the increasing potential in targeted direct marketing in

---

[65] Information Commissioner Office, 'Data Protection Technical Guidance: Radio Frequency Identification' <http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/radio_frequency_indentification_tech_guidance.pdf> accessed 18 November 2009.

[66] Ibid 5-6.

[67] Ibid.

[68] Ibid 5.

[69] For further issues regarding RFID and identity management, see: European Technology Assessment Group, European Parliament, 'RFID and Identity Management in Everyday Life: Striking the balance between convenience, choice and control' (2007) IPOL/A/STOA/2006-22. Available at: < http://www.europarl.europa.eu/stoa/publications/studies/stoa182_en.pdf> accessed 18 November 2009.

[70] For further discussion, See: Ari Juels, 'RFID Privacy: A Technical Primer for the Non-Technical Reader' in Katherine J. Strandburg and Daniela Stan Raicu (eds), *Privacy and technologies of identity: a cross-disciplinary conversation* (Springer 2006) 63-64.

comparison with bar code AIDC technologies.[71]

Additionally, to complete the picture, there is a dramatic move to the use of biometrics in ubiquitous ICT developments, e.g., RFID. It is noted that those benefits and risks mentioned in both biometric and RFID technologies may extend when using biometric technology in conjunction with RFID – not only in those discussed technique problems and social concerns, but also in privacy and data protection regimes, which will be introduced in next section.

2.4 Biometrics, RFID, and Data Protection: Relationships, Concerns and Examples

Despite there being a number of social concerns regarding biometrics and RFID, it is not surprising that the major concern has centred on privacy and data protection aspects.[72] In light of data protection concerns regarding biometrics and RFID, two questions will be addressed: (1) whether biometric data is subject to data protection law, particularly under the definition of Directive 95/46/EC and its local implications; (2) whether biometric data is a type of sensitive personal data.

2.4.1 Biometric Data and Concepts of (Sensitive) Personal Data

[71] Parliamentary Office of Science and Technology (n 52) 3-4.

[72] Article 29 Data Protection Working Party, *Working Documents on Biometrics*. Article 29 Data Protection Working Party, *Opinion 3/2012 on Developments in Biometric Technologies* 8.It has been argued that there are three information regime may be threaded together: the privacy regime, processing of personal data regime, and the confidentiality regime. See: Roger Brownsword, 'Consent in Data Protection Law: Privacy, Fair Processing and Confidentiality' in Serge Gutwirth and others (eds), *Reinventing Data Protection?* (Springer 2009) 83-110.

2.4.1.1 Does Biometric Data fall within the Scope of Personal Data?

The concept of personal data, which specifies the scope of personal data, has a profound impact on the issues with regard to 'Identity Management in the context of e-Government and e-Health, as well as in the RFID context.'[73]

According to Article 2(a) of the Data Protection Directive, personal data is defined as 'any information relating to an *identified or identifiable natural person* ('data subject')…'[74] (emphasis added). Recital 26 of the Directive, meanwhile, states that 'the principles of protection must apply to any information concerning an identified or identifiable person…' In determining whether a person is identifiable, furthermore, the Directive specifies that 'an identifiable person is one who can be identified, *directly or indirectly*, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social *identity*' (emphasis added).[75] It is further explained by Recital 26 that 'account should be taken of all the *means likely reasonably* to be used either by the controller or by any other person to identify the said person.' (Emphasis added)

Moreover, the 2012 proposal of the EU General Data Protection Regulation, in line with opinion WP 136, proposes in Article 4 (1) that ''data subject' means an identified natural person or a natural person who can be identified, directly or indirectly, by means reasonably likely to be used by the controller or by any other natural or legal person, in particular by reference to an identification number, location data, online identifier or to one or more factors specific to the physical, physiological,

[73] Article 29 Data Protection Working Party, *Opinion 4/2007 on the Concept of Personal Data* (No 01248/07/EN, WP136, 2007) 3.
[74] The same definition is also stated both in Article 2 (a) of the 1981 Data Protection Convention and Section 1 (b) of the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (the OECD Guidelines).
[75] Article 2(a) of Directive 95/46/EC.

genetic, mental, economic, cultural or social identity of that person.'[76]

With these definitions and explanations in mind, it seems to be much easier to answer the first question according to characteristics of biometric data. The WP29, therefore, suggests that 'measures of biometric identification or their digital translation in a template form in *most* cases are personal data' (emphasis added).[77] Furthermore, it is arguable that the feature of automaticity places biometric systems within the scope of the main legal regulations that this thesis is going to focus on, e.g., Directive 95/46/EC, [78] Directive 2002/58/EC, [79] the 1981 data protection Convention, [80] the Data Protection Act 1998 of the UK (DPA), [81] the Computer-Processed Personal Data Protection Law of Taiwan (CPDPL), [82] and the Personal Data Protection Law (PDPL).[83]

---

[76] However, as regards Recital 24 of the proposed general Regulation, it is argued by the WP29 that the Recital 'might lead to an unduly restrictive interpretation of the notion of personal data in relation for instance to IP addresses or cookie IDs.' Article 29 Data Protection Working Party, *Opinion 01/2012 on the Data Protection Reform Proposals* (No 00530/12/EN, WP191, 2012) 9.

[77] Article 29 Data Protection Working Party, *Working Documents on Biometrics* 5.

[78] Article 3.1 of Directive 95/46/EC addresses that 'This Directive shall apply to the processing of personal data wholly or partly by automatic means, and to the processing otherwise than by automatic means of personal data which form part of a filing system or are intended to form part of a filing system.'

[79] Article 1.2 of Directive 2002/58/EC stands that 'The provisions of this Directive particularise and complement Directive 95/46/EC for the purposes mentioned in paragraph 1. Moreover, they provide for protection of the legitimate interests of subscribers who are legal persons.'

[80] Article 3.1 of 1981 data protection convention gives that 'The Parties undertake to apply this convention to automated personal data files and automatic processing of personal data in the public and private sectors.'

[81] Article 1.1 of the DPA (of the UK): '…"data" means information which— (a) is being processed by means of equipment operating automatically in response to instructions given for that purpose; (b) is recorded with the intention that it should be processed by means of such equipment; (c)is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system, or (d)does not fall within paragraph (a), (b) or (c) but forms part of an accessible record as defined by section 68.'

[82] Articles 3.1 and 3.2 of the CPDPL: 'the term "personal data" means the name, date of birth, uniform number of identification card, special features, finger print, marriage, family, education, profession, health condition, medical history, financial condition, and social activities of a natural person as well as other data sufficient to identify the said person.' 'the term "personal data file" means a collection of personal data stored in a electromagnetic recorder or other similar media for specific purposes.'

[83] Articles 2.2 and 2.3 of the PDPL: 'Personal data: the name, date of birth, I.D. Card number, passport number, characteristics, fingerprints, marital status, family, education, occupation, medical record, medical treatment, genetic information, sexual life, health examination, criminal record, contact information, financial conditions, social activities and other information which may be used to identify a natural person, both directly and indirectly;' 'Personal data file: A collection of personal information

However, Recital 26 of the Data Protection Directive reads that '…the principles of protection shall not apply to data rendered anonymous in such a way that the data subject is no longer identifiable…' The description of 'no longer identifiable' has been given by the WP29 that '[i]n cases where biometric data, like a template, are stored in a way that *no reasonable means* can be used by the controller or by any other person to identify the data subject, those data should not be qualified as personal data.'[84] (emphasis added)

Nonetheless, this sort of situation, to use the phrase coined by Rejman-Greene, is 'likely to be relatively rare.'[85] In his opinion, there are seven requirements to be met.[86] Only after *all* these requirements are satisfied, could it *possibly* be considered that non-identifiability is achieved. This is because, per Article 2(a) and Recital 26, if there is any possibility that *anyone could reasonably relink* the datasets, those coded data should not be considered as anonymous.[87]

It is noted, in this regard, that anonymisation is by no means a privacy-offering panacea. Indeed, the 'easy reidentification result' has been observed by Ohm in his

---

built to allow information retrieval and management by *automatic or non-automatic* measures;' (emphasis added)

[84] Article 29 Data Protection Working Party, *Working Documents on Biometrics* 5.

[85] Rejman-Greene (n 38) 344.

[86] Ibid 344-345. These addressed conditions are:

1. The identity of a previously enrolled individual is only represented by a "one way" template without any possibility of reconstruction of the original record;
2. The template could also be generated by a sufficient number of other subjects in the population;
3. The template is stored on a token held by the end user;
4. The comparison, at verification, of the output of the sensor with the template, is made on the token itself;
5. All images and records relating to the enrolment are securely disposed of at the time of enrolment;
6. No other data is available that, combined with the biometric data, could link the user uniquely to a template; and
7. The backup alternative, in case of failure of the biometric, does not expose the biometric to a process whereby a subsequent verification could reveal the person's identity.

[87] Deryck Beyleveld, 'Data Protection and Genetics: Medical Research and the Public Good' (2007) 18 King's Law Journal 280-283.

article concerning the failure of anonymisation.[88] Such failure, which is made more likely by recent technological advances in reidentification, may require modification of what is considered to be personal data.[89] Accordingly, easily re-identifiable data is within the scope of personal data.[90]

A similar opinion is reached in the report released by the Consultative Committee of the 1981 Data Protection Convention (T-PD) regarding the collection and processing of biometric data.[91] It is argued in this document that '[t]he collection of biometric data can only take place under certain circumstances regarding, for example, the time and the place of their collection', and '[t]hese circumstances always reveal information about the data subject being the source of the biometric data.'[92] The T-PD therefore concludes that:

> The Committee finds it unnecessary to decide whether biometric data are personal data in themselves or whether this is only the case under certain circumstances. It is of the opinion that as soon as biometric data are collected with a view to automatic processing there is the possibility that these data can be related to an identified or identifiable individual. In those cases the Convention applies.[93]

Overall, except in rare cases which the data subjects are no longer identified by a reasonable measure, biometric data falls within the scope of personal data. Moreover,

---

[88] Paul Ohm, 'Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization' (2010) 57 UCLA Law Review 1716. For additional discussion on anonymisation and reidentification techniques, see: ibid 1711-1727.
[89] Ibid 1731-1745.
[90] For further discussion on identifiable and identified personal data, see: section 8.3.1.
[91] The Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, 'Progress Report on the Application of the Principles of Convention 108 to the Collection and Processing of Biometric Data' (*T-PD*, 2005) <http://www.coe.int/t/e/legal_affairs/legal_co-operation/data_protection/documents/reports_and_studies_of_data_protection_committees/2Biometrics_2005_en.pdf> accessed 13 February 2010.
[92] Ibid para. 51.
[93] Ibid para. 52.

in the light of the advanced technologies causing the easy reidentification result, I suggest that due to the development of new technologies that may affect data protection,[94] it is essential to review the current data protection legal framework.[95]

2.4.1.2 Is Biometric Data a Type of Sensitive Personal Data?

Article 8(1) of the Data Protection Directive specifies that the processing of five special categories of personal data shall be prohibited unless exemptions stated by Articles 8(2) and 8(3) apply. These categories are the processing of personal data relating to the data subject's, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, or health or sex life.

It seems to be obvious that facial images, which are essential to achieve the measurability demand of a facial-scan system, will reveal the data subject's racial or ethnic origin, or at least, will provide indications of it. Accordingly, images for such type of biometrics should be considered as sensitive data. However, can the processing of mere indication of sensitive personal data, which are processed in low threshold applications (e.g., facial images, voice and signatures) to be conclusive as to its nature for the purpose of the regulation? It has been claimed by certain European countries that:

---

[94] Yue Liu, 'Identifying Legal Concerns in the Biometric Context' (2008) 3: 1 Journal of International Commercial Law and Technology 47-48. Also, Neil Robinson and others, *Review of the European Data Protection Directive* (Technical Report, 2009).

[95] See section 8.3. In this respect, it is noted that the proposed 2012 EU General Data Protection Regulation has introduced a definition of biometric data in Article 4(11). It states that: ''biometric data' means any data relating to the physical, physiological or behavioural characteristics of an individual which allow their unique identification, such as facial images, or dactyloscopic data.' However, the WP29 finds that, as biometric data are used in both identification and authentication purposes, the wording in Article 4(11) should be amended as '…are unique for each individual specifically…' Article 29 Data Protection Working Party, *Opinion 01/2012 on the Data Protection Reform Proposals* 10.

> '…Article 8.1 arguably applies to the processing of an image of a person, since that image will always "reveal" the ethnic or racial origin of the person, unless he or she is masked or otherwise heavily disguised…' and '…such essentially incidental "revelations" of the characteristics described in Article 8.1 do not amount to sensitive data for *the purposes of the Article*.' (emphasis added)[96]

Therefore, it may be asserted that those facial images should not be considered as sensitive data – at least not at the early stage before being saved into a template[97] or a RFID tag.

Nonetheless, this is not the whole story. It is worth noting that the same document further suggested that those special categories 'where they clearly describe intimate personal characteristics and their processing is particularly likely to infringe fundamental freedoms or privacy…' should 'in principle not be processed.'[98] Indeed, we need to look at the purpose of the processing of personal data. In this regard, it has been argued that facial images *for processing of biometrics*, which describe intimate characteristics of those data subjects and *aim to process sensitive data* (e.g., the identity management), constitute sensitive personal data.[99] On the basis of the 2012 EU proposal of General Data Protection Regulation, furthermore, as facial image is clearly listed as a type of biometric data (Article 4(11)), and it is referred that biometric data *presents specific risks to the rights and freedoms of data subjects* (Article 33(2)(d)), I argue that facial images, in particular for the propose of processing of biometrics, should, as the above document addressed, in principle not

[96] Department of Constitutional Affairs, 'Proposals for Amendment made by Austria, Finland, Sweden and the United Kingdom: Explanatory Note' <http://www.dca.gov.uk/ccpd/dpdamend.htm> accessed 18 January 2010.
[97] Rejman-Greene (n 38) 345-346.
[98] Department of Constitutional Affairs, annex: Proposed Amendments to Data Protection Directive (95/46/EC), special categories of data.
[99] Cf. Peter Carey, *Data Protection: A Practical Guide to UK and EU Law* (2nd edn, OUP 2004) 87.

be processed.

On the other hand, high threshold applications, such as DNA data for DNA-scan systems, can surely reveal racial or ethnic origins. DNA data, which contains genetic material, reveals not only racial or ethnic origin but also health information, and has been rightly argued to be subject to data protection law.[100] Furthermore, other types of biometrics such as fingerprints, hand and palm geometry, iris recognition and retina recognition, as suggested above, may reveal health and sex life information. Therefore, those kinds of biometrics, in most contexts, should be considered as sensitive data under the Directive and thus should merit a higher degree of protection under the data protection law regime.

However, it seems that to directly treat biometric data as a form of sensitive data in general has not received much support.[101] It might be said that biometric information *per-se* does not directly reveal health information – it needs a technological shift in order to identify it.[102] Nonetheless, I argue that, if there is any possibility to reasonably *identify or relink/ re-identify* biometric data and relevant sensitive information such as health, racial or ethnic origin, it should be considered as sensitive data. This is because, as we shall see in the latter part of this thesis, the scope of right to privacy should be interpreted broadly.[103]

2.4.2 Concerns over Data Protection

Since both of the preconditioned questions are given positive answers, this section

[100] Beyleveld (n 87) 277-283.
[101] Liu (n 94) 47.
[102] Ibid.
[103] Section 4.3.2.

returns to its focus on the data protection concerns over biometrics and RFID. As remarked by Koops and Leenes:

> …In the vast majority of technologies developed and used in real life, its influence is to the detriment of privacy. That is, technology often has the side-effect of making privacy violations easier…
>
> …Examples in law enforcement and e-government show technology offers increasing opportunities for large-scale monitoring – from intercepting all telecommunications…to monitoring the movements of people. In the private sector, technology enables more control of people, from workplace and transaction monitoring to personalization of consumer relationships, with new applications like *facial recognition and RFID monitoring* looming ahead… (emphasis added) [104]

Indeed, biometric and RFID technologies do attract certain growing privacy and data protection concerns. In this regard, these concerns reflect different contexts of data protection principles for the use of new technologies respectively: (1) processing sensitive data; (2) processing in a way compatible with the specified original purposes; (3) processing in an adequate, relevant and not excessive way in relation to the purposes; and (4) processing in a mass-scale way managed by national or supranational databases.

2.4.2.1 Information about Human Bodies

With the ‘life measuring’ nature of biometrics, it is an essential feature of biometric

[104] Bert-Jaap Koops and Ronald Leenes, ‘'Code' and the Slow Erosion of Privacy’ (2005) 12 Michigan Telecommunications and Technology Law Review 245.

technologies to process personal data containing information about human bodies. As we have seen, biometric data which involves personal health data or data involving sex life, in most contexts, is a sort of sensitive personal data. With this in mind, the first question concerns the data subject's explicit consent. For example, according to Article 8(2)(a) of the Data Protection Directive, consent is the very first justification regarding the principle of prohibiting the processing of special categories of data. Moreover, the ECtHR has held that processing sensitive personal data without explicit consent will engage Article 8(1) of the ECHR.[105] In this regard, with explicit consent made by the data subject, no further justification is required.[106]

However, it is possible for some biometric traits or measures to be taken and processed without explicit consent, or even the data subject's knowledge, in a biometric system. Examples of possible methods include collecting facial images or voice records from CCTV surveillance cameras and microphones, collecting fingerprints, hand and palm prints from the surface of something or somebody, and collecting DNA samples from body tissues in a crime scene. Also, it is possible for researchers to link medical information revealed by biometric data to particular biometric patterns. Moreover, biometric data which is stored in a RFID tag could also be copied or cloned without explicit consent.

These examples violate the principle of security processing of personal data as required, for example, by Article 17 of the Data Protection Directive. Since consent is inclusive of the stage of collecting the biometric data, it is also arguable that consent plays a central role on the data protection principle of fair and lawful processing relating to data quality.[107] In this case, if there is no explicit consent made by the data

[105] See: *Z. v Finland* (1998) 25 EHRR 371. Also, *MS v Sweden* (1999) 28 EHRR 313.
[106] Beyleveld (n 87) 284.
[107] Article 6.1 (a) of the Data Protection Directive: Member States shall provide that personal data

subject as the gatekeeper of the relevant rights, then justification must be found to prevent breaching the rights.[108]

2.4.2.2 Function Creep

'Function creep,' i.e., further unintended or unnecessary processing of personal data in a way incompatible with the original purpose for which it was collected, has been emphasised as one of 'the most significant informational privacy concerns' by the RAND institution.[109] Function creep happens not only with the knowledge or consent of data subjects, but also occurs without the active involvement of data subjects. In this regard, the lack of transparency of collecting and processing personal data should be considered. In fact, the transparency problem of RFID systems has been identified by the EDPS as one of the five privacy and data protection issues in RFID deployment.[110] This is a negative impact on the trust relationship between data controllers and data subjects.

The development of interoperability between biometric/ RFID systems further extends the possibility of function creep. It has been observed that the application of biometrics presents 'a greater potential for function creep'[111] than traditional authentication methods could achieve. One of the significant threats comes from the consent issue. This is because the most commonly used biometrics of individuals, e.g.,

---

must be: 'processed fairly and lawfully;'

[108] Beyleveld (n 87). For further discussion regarding such justifications, see section 6.4.

[109] Woodward and others, *Army Biometric Applications: Identifying and Addressing Sociocultural Concerns* 3.

[110] These five basic privacy and security issues distinguished by the EDPS are: identification of the data subject, identification of the controller(s), the decreased meaning of the traditional distinction between the personal and public sphere, the size and the physical properties of RFID-tags, and the lack of transparency of the processing. See: The European Data Protection Supervisor paras. 20-27.

[111] See, *Woodward and others, Army Biometric Applications: Identifying and Addressing Sociocultural Concerns* 30.

facial images, voice, signatures and other low threshold applications, which are thought as 'hardly' to be changed or discarded, are regularly exposed and recognised in public and.[112] This increases the possibility of collecting and processing biometrics of individuals without the active involvement of data subjects (through a RFID system).

Function creep, by its nature, raises an obvious problem in that it goes against the principle of obtaining personal data for specific, explicit and lawful purpose(s) and processing it in a compatible manner.[113] It also goes against an important principle of the data protection law regime: the principle of proportionality. In this light, the WP29 clearly points out that:

> 'an evaluation of the respect for proportionality and the respect for legitimacy is necessary, taking into account the risks for the protection of fundamental rights and freedoms of individuals and notably whether or not the intended purpose could be achieved in a less intrusive way. Proportionality has been the main criterion in almost all decisions taken until now by the Data Protection Authorities on the processing of biometric data.'[114]

2.4.2.3 Tracking and Profiling

Due to the 'internet of things' characteristic of RFID technology, the interoperability

[112] Ibid 30-31.
[113] Article 6.1 (b) of Directive 95/46/EC: Member States shall provide that personal data must be: '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.'
[114] Article 29 Data Protection Working Party, *Working Documents on Biometrics* 6.

between biometric/ RFID systems and other different information databases presents a particular type of function creep: the abuse of tracking or profiling personal data. The definition of tracking is given as 'the ability to monitor in real time an individual's actions or to search databases that contain information about these actions,'[115] or 'the possibility of linking different transactions to build profiles.'[116] Tracking refers to track/ trace individuals' movements or locations, which is in close relation to one's spatial privacy. For example, facial-scan biometric system with a RFID, CCTV, GSM, or GPS system could identify and locate individuals easily without consent.

On the other hand, 'profiling' means to profile individuals' behaviour, which relates to one's information privacy by linking individuals to personal data. Profiling could be carried out through data mining. For example, biometric database with passengers' record could figure how regular one visits a particular place. Briefly, tracking asks the question of 'where was/is she/he?' and profiling asks 'why she/he was/is there?'

In this case, data protection concerns in relation to function creep including the consent issue, purpose principle, principle of proportionality, and the transparency/ trust issue must be considered. Moreover, tracking and profiling through biometric data could allow data controllers to build a clear image of personality in an all-round manner of a data subject. Although the action of collecting and processing personal data is, or at least may be, for the original purpose, it must be done in an adequate, relevant and not excessive manner. Accordingly, *unless such a purpose aims to protect an absolute right and is the proportional method of achieving the goal*, it can hardly be accepted that an overall or any unnecessary extent of the 'image of an

[115] Woodward and others, *Army Biometric Applications: Identifying and Addressing Sociocultural Concerns* 24-25.
[116] Sethi (n 10) 133.

individual's personality' is needed for any purpose.

2.4.2.4 National/ International Scale Databases

Biometric and RFID technologies have been applied in both public and private spheres on a massive scale rapidly. Promoted by the International Civil Aviation Organisation (ICAO), passports with RFID tags containing biometric data and other personal identification data are a good example of this trend. This trend draws social concerns such as public trust on legal and political procedures, and of course, data protection concerns.

Since both the right to privacy and the data protection rights are not absolute rights, it is commonly argued by governments or international organisations that those technologies are deemed to be necessary to uphold some public good such as national security, public security, and investigation and prevention of crime. Therefore, it is not surprising that the tendency of building national/ international biometric databases in order to take surveillance on *every* potential criminal is preferred due to the efficiency of protecting above securities and prevention of crime. In this regard, the increasing trend of collecting and processing personal data on a wider range of data subject calls for a series of considerations. It has been indicated in a report commissioned by the UK Information Commissioner's Office, that the 'significant extension of the role of the police from their traditional tasks' is now 'typically intelligence-led' – which involves the trend of collecting and processing personal data on a 'wider range of data subject.'[117] Moreover, the specific risks of 'reuse of such data for incompatible

[117] Foundation for Information Policy Research, *Paper No. 5: Conclusions & Policy Implications* (UK Information Commissioner Study Project: Privacy & Law Enforcement, 2004) 1-3.

purposes' are also increased.[118] Under such circumstances, restrictions on certain data protection principles including principle of obtaining an explicit consent, the principle of processing personal data fairly and lawfully, and certain information rights of data subject, will be applied.

Indeed, with respect to the rights-balancing issue between the right to privacy and data protection and other collective interests, it is observed by Paul de Hert that

> [p]rivacy and human dignity must preserve the roots of the individual's autonomy against outside steering or against disproportionate power balances in vertical, but also in horizontal power relations.[119]

Therefore, there is a need to deal with the question stems from the interference on the individual's autonomy and free will of choice, particularly in a *unbalanced* power relations which threatens not only human rights and freedoms, but also 'the very nature of our society.'[120] Before dealing with this question, it is helpful at the outset to offer some real-life examples of specific technologies to reflect on the current and future circumstances.

2.4.3 Examples

Three main themes are provided here as examples of the ways in which new technologies affecting our daily lives: (1) the private sector; (2) health sector; and (3)

---

[118] Article 29 Data Protection Working Party, *Opinion 3/2012 on Developments in Biometric Technologies* 15.
[119] Paul de Hert, 'Biometrics at the Frontiers: Assessing the Impact on Society' <http://cybersecurity.jrc.ec.europa.eu/docs/LIBE%20Biometrics%20March%2005/iptsBiometics_FullReport_eur21585en.pdf> accessed 29 July 2010.
[120] Ibid 91.

policing sector.[121]

2.4.3.1 Private Life

Within the private business sector, biometric techniques are commonly used in daily electric facilities such as laptops, mobile phones, premise gate controllers, and even campus libraries.[122]

With regard to RFID technology, the EU Commission reports[123] that the primary cost of RFID tags is decreasing as production rises thus allowing for a wider usage. Retailers could, therefore, apply this technology to keep shelves stocked, to better account for inventories, and to reduce theft and loss with less labour cost and errors. Other current practical applications include electronic payment, supply chain management, animal tracking, and data conveying in hostile environments.[124] RFID technology is also applied in data processing fields such as access control and payment facilities.

Moreover, using biometrics in conjunction with RFID applications to replace keys as a method of identification or verification is common. This is applied not only

[121] There are other methods to present similar examples such as using the scenario methodology. See: Ioannis Maghiros and others, 'Biometrics at the Frontiers: Assessing the Impact on Society' <http://cybersecurity.jrc.ec.europa.eu/docs/LIBE%20Biometrics%20March%2005/iptsBiometics_FullReport_eur21585en.pdf> accessed 29 July 2010. For examples and references to specific biometric systems and technologies, e.g., vein pattern, fingerprints, facial recognition, voice recognition, signature biometrics, DNA and their combined uses, see: Article 29 Data Protection Working Party, *Opinion 3/2012 on Developments in Biometric Technologies* 16-27.

[122] E.g., Information Commissioner Office, 'The Use of Biometrics in Schools' <http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/fingerprinting_final_view_v1.11.pdf> accessed 18 November 2009. It is also described by Article 29 DP working party that 'the use of biometrics in school libraries can make children less aware of the data protection risks that may impact upon them in later life.' Article 29 Data Protection Working Party, *Working Documents on Biometrics* 2.

[123] COM (2007) 96 final at 3.

[124] For a detailed description, see: *Parliamentary Office of Science and Technology* (n 52) 2.

in tangible spaces but also digital spaces such as the internet. The former type in relation to personal data, as previously discussed, is regulated by the Data Protection Directive in EU. Specific types of applications of such technologies may be at the same time regulated by further EU legislation. Applying biometrics in schools, especially for tracking underage children, for instance, is a further concern for the public. It is pointed out by the Information Commissioner's Office (UK), for example, that two objections may arise from applying biometric in schools: stigmatisation and an attempt to teach children that giving up crucial personal data to those in authority is normal and acceptable.[125]

The latter type can be exemplified by electronic/ digital biometric signatures[126] which are referred to any electronic data that carries the intent of a signature in order to satisfy digital accesses or payments. It is rapidly used in online shopping in the digital era. This falls not only within the scope of Directive 1999/93/EC,[127] but also the Data Protection Directive, Directive 2005/58/EC[128] and Directive 2006/24/EC[129] which amended Directive 2002/58/EC; the common purpose of last two directives is to harmonise Member States' provisions concerning the obligations of the providers of 'publicly available electronic communications services or of public

[125] Information Commissioner Office, 'The Use of Biometrics in Schools'.
[126] According to Article 2(1) of Directive 1999/93/EC, 'electronic signatures' means 'data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication.'
[127] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures (OJ L 13 of 19/1/2000).
[128] 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 (OJ L 201, 31/07/2002, 37-47). This Directive replaces Directive 97/66/EC, which was concerning on the processing of personal data and the protection of the privacy in the telecommunication sector.
[129] 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 L 105, 13/04/2006, 54-63).

communications networks with respect to the retention' of such personal data.'[130]

2.4.3.2 Health/ Medical Sector

With the sensitive nature of medical care, positive and accurate identification is essential. It is therefore common for health networks to propose massive applications of biometric technologies and RFID tags. Particular disadvantages, however, can be identified by applying biometric associated technologies in this sector. For example, 'fingerprints will not work in environments where users wear latex gloves, face recognition will not work with surgical masks, and voice recognition will not work in noisy environments.'[131] Another example is the health card with personal biometric data and RFID tags, which may involve both private insurance firms and public authorities.

2.4.3.3 Policing Sector

To improve public safety and convenience, biometric technologies are now applied in various fields such as military services,[132] migration controls,[133] and national ID cards

[130] Article 1 of Directive 2006/24/EC.
[131] Maghiros and others (n 121) 108.
[132] Army forces have used biometrics as one of the solutions to take care of needs of a security and safety way to control access to their systems in times of both war and peace. See: Woodward and others, *Army Biometric Applications: Identifying and Addressing Sociocultural Concerns*.
[133] It is exactly due to these mentioned advantages that since 11 September 2001, biometrics has become a 'powerful weapon' to defend states borders and improve nation security. Some developed countries are now using biometrics in their migration management. See: International Organization for Migration, *Biometrics and International Migration* (International Organization for Migration 2005). For example, the UK government is now issuing biometric ID cards and visas to foreign students, employers, and workers. This card will also show information about the identity of the holder and details such as the length of their leave to stay in the UK and whether they are entitled to work. See: <http://www.ukba.homeoffice.gov.uk/managingborders/idcardsforforeignnationals/> accessed 18 November 2009.

policies.[134]

Similarly, RFID applications are now also commonly used and their diffusion is increasing at a very rapid rate. For example, the ICAO is now promoting a set of global passport standard endorsing the deployment of RFID tags in passports.[135] In this respect, the EU has issued Regulation EC 2252/2004,[136] later amended by Regulation EC 444/2009,[137] to ensure the use of biometric passports meet certain security standards. Article 4(3) of Regulation EC 444/2009, which aims to avoid the function creep problem, states that biometric features in passports and travel documents shall only be used for verifying two specific aspects: 'the authenticity of the passport or travel document' and 'the identity of the holder by means of directly available comparable features when the passport or travel document is required to be produced by law.'

2.5 Summary

The chapter has addressed key terms, the promised benefits and the potential risks of biometric and RFID applications respectively.

---

[134] Some countries, e.g., China (beginning with Shenzhen City), issued biometric ID cards (with lots of other sensitive data such as personal reproductive history) to their citizens. See: < http://www.nytimes.com/2007/08/12/business/worldbusiness/12security.html?_r=2&ei=5065&en=2d7edb61ed1&oref=slogin> accessed 18 November 2009. The UK is now issuing biometric ID cards to their citizens. See: < http://www.direct.gov.uk/en/Governmentcitizensandrights/Identitycards/DG_174258> accessed 18 November 2009.

[135] Katherine Albrecht, 'How RFID Tags Could Be Used to Track Unsuspecting People' *Scientific America Magazine* (New York, 19 August, 2008) < http://www.scientificamerican.com/article.cfm?id=how-rfid-tags-could-be-used> accessed 18 November 2009.

[136] Council Regulation (EC) No 2252/2004 of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States.

[137] Regulation (EC) No 444/2009 of the European Parliament and of the Council of 28 May 2009 amending Council Regulation (EC) No 2252/2004 on standards for security features and biometrics in passports and travel documents issued by Member States.

With respect to the benefits of the advanced technologies at hand, convenience and safety concerns are commonly shared. For biometric applications, particular concerns mainly focus on issues related to sensitive personal data. It has been argued that, except in rare cases in which the data subjects are no longer identified by reasonable methods, biometric data falls within the scope of personal data. In connection with the question of whether biometric data is a sort of sensitive personal data, I adopt the idea that if there is any possibility to reasonably *identify or re-identify* biometric data and relevant sensitive information such as health, racial or ethnic origin, the answer should be in the affirmative. As regards RFID applications, on the other hand, the focus should be on concealed tracking and profiling problems. Attention was drawn to four data protection concerns: information about human bodies, function creep, profiling and tracking biometric data, and databases in a national or international mass-scale were then presented, which share a common concern over the potential interferences with individuals' *free will*. These data protection concerns present four themes worth noting: the concept of privacy, consent, trust, and interest-balancing issues between public goods and individual interests. These four themes will be examined in detail throughout the thesis.

Chapter 3

Introducing an Applicable Theoretical Framework:

The Principle of Generic Consistency and Its Justification

3.1 Introduction

An adequate theoretical framework is essential to approach the research question of this thesis. This is because, in order to answer the research question, the relevant competing rights and interests must be reconciled on the basis of a criterion to determine how one can identify the rights to be protected and understand the values of the rights. The proposed theoretical framework is the moral theory of Alan Gewirth – the Principle of Generic Consistency, stating that **agents must act in accord with the generic rights of all agents**.[1]

This chapter is organised in eight sections. The outline of the PGC will be presented in section 3.2. Two main formulations of the arguments elaborating the PGC will then be offered in sections 3.3 and 3.4. The first argument is based on Gewirth's own contribution *Reason and Morality*, arguing that **agents contradict that they are agents if they do not accept that the PGC is the supreme principle governing all of the permitted actions**.

An alternative argument is presented by a Gewirthian scholar Deryck Beyleveld

[1] Alan Gewirth, *Reason and Morality* (University of Chicago Press 1978) 135. Also, Deryck Beyleveld and Roger Brownsword, *Human Dignity in Bioethics and Biolaw* (OUP 2001) 70.

in his article *Legal Theory and Dialectically Contingent Justifications for the Principle of Generic Consistency*.[2] He argues that an agent contradicts its[3] acceptance that human beings are equal in human rights if it does not grant the PGC a similar status, i.e., 'interpret and give effect to human rights in way consistent with the PGC.'[4] In this case, **anyone (or any legal system) who recognises human rights (with the idea that human beings are equal in dignity and rights) must grant the PGC a similar status or contradict acceptance of such rights**. Therefore, the enforcement machinery of any part of a network of international human rights treaties of universal or regional application, e.g., the ICCPR, the ECHR and the European Union Charter of Fundamental Rights, must be interpreted in conformity to the PGC. Overall, these two arguments are capable of showing the PGC as the governing principle in appeals to human dignity and human rights in all ethics and law, including in the data protection regime.[5]

Section 3.5 aims to provide the content of agency rights under the PGC. Section 3.6 will then show a logical consistency rule which is compatible with an order whereby some interests/rights are overridden by others.

Lastly, it must be noted that Gewirthian moral theory 'runs against the current

[2] Deryck Beyleveld, 'Legal Theory and Dialectically Contingent Justifications for the Principle of Generic Consistency' (1996) 9 Ratio Juris 15-41.

[3] It has been criticised by Singer that the use of the pronoun 'it' referring to an agent is 'barbaric.' Marcus G. Singer, 'Gewirth, Beyleveld, and Dialectical Necessity' (2000) 13 Ratio Juris190. However, it must be noted that the PGC is directly about agents rather than human beings. Deryck Beyleveld, 'A Reply to Marcus G. Singer on Gewirth, Beyleveld and Dialectical Necessity' (2002) 15 Ratio Juris 458. By reading section 3.2.3 of this thesis, it should be noted that there is no such a requirement to ask agents to be human or any gender beings. Accordingly, as Beyleveld puts it, this terminology considers nothing about reasons of 'political correctness' or mere preference. Indeed, for some applications of this theoretical framework, the use of 'it' can function as avoiding suggesting that agents are necessarily male or female. Shaun D. Pattinson, *Influencing Traits Before Birth* (Ashgate Publishing 2002) 3. In this regard, I may sometimes use the pronoun 'it/ he/she.' This is because there are (limited) chances for agent to be human beings, in particular under the situation of discussing the right to privacy and data protection in the later chapters.

[4] Deryck Beyleveld, 'The Principle of Generic Consistency as the Supreme Principle of Human Rights' (2012) 13 Human Rights Review 1.

[5] Beyleveld and Brownsword, *Human Dignity in Bioethics and Biolaw* 69.

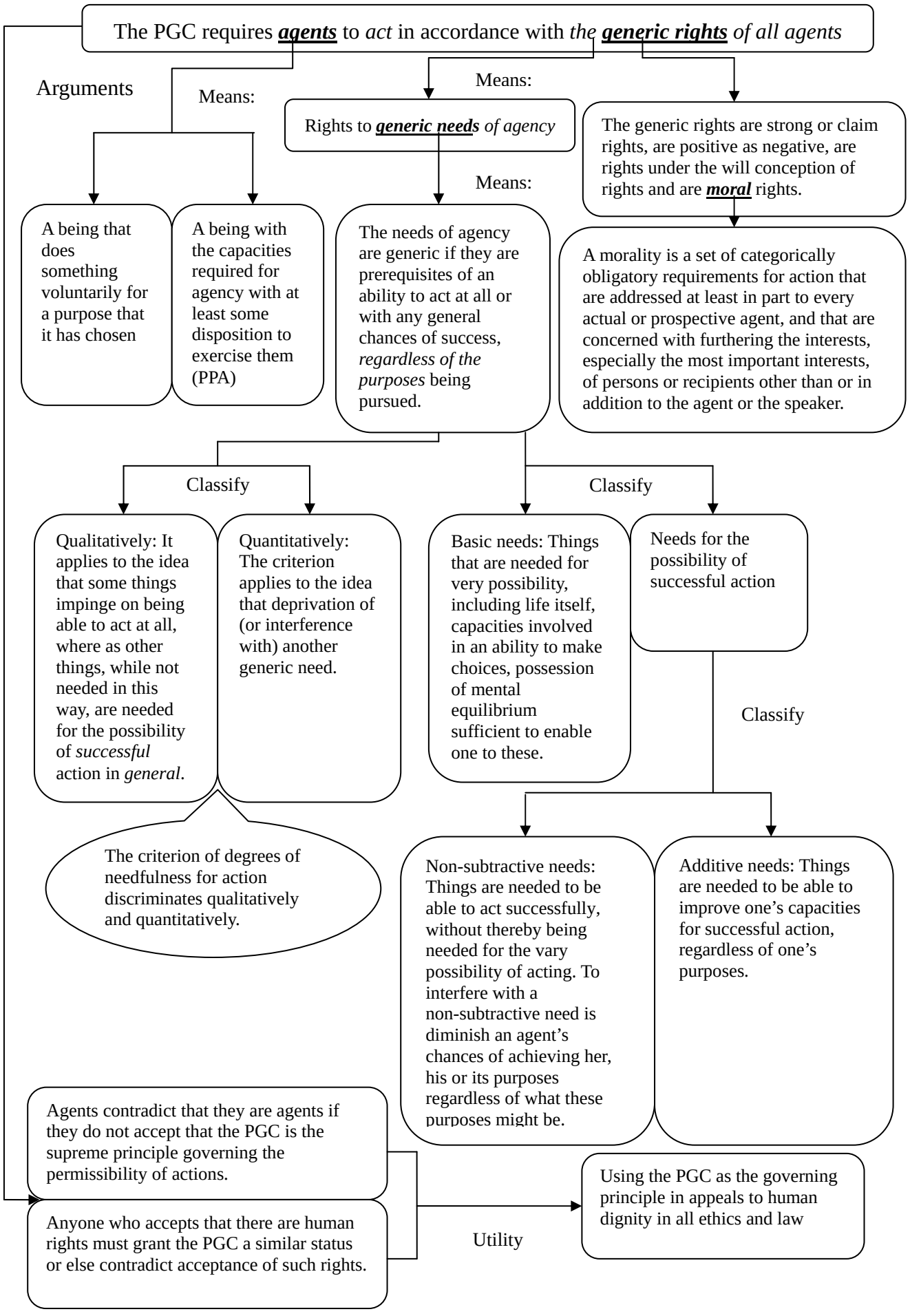
trend of modern philosophy.'[6] This chapter, in this regard, must seek to provide convincing reasons for the adoption of the PGC. Moreover, we shall attempt to respond to the objections raised against the PGC. These two goals shall be achieved in section 3.7, following by a summary in section 3.8.

3.2 The Outline of the Principle of Generic Consistency

It is claimed by Gewirth that **the PGC requires agents to act in accordance with the generic rights of all agents**. This statement combines two major components: 'the formal consideration of consistency' and 'the material consideration of rights to be the generic features or goods of action.'[7] To present a brief overview of this supreme principle, the following map[8] tries to unpack the major terms and notions of the PGC.

[6] Pattinson (n 3) 3.
[7] Alan Gewirth, *The Community of Rights* (The University of Chicago Press 1996) xi.
[8] This map is based on Beyleveld and Brownsword's contribution: Beyleveld and Brownsword, *Human Dignity in Bioethics and Biolaw* 70-72.

The Map of the Principle of Generic Consistency



The Agent

According to Gewirth, an agent is 'an actual performer of actions or a prospective purposive performer of actions who does (perform) something voluntarily for a purpose that it has chosen.'[9] It refers to a being with capacity to control its ability of doing something (X) through its unforced, informed choice,[10] so as to try to achieve its purpose (E).[11] It should be noted that E should be treated by an agent as the reason for its action[12] since an agent is able to act 'through consideration of characteristics understood to pertain to the possible address of practical precepts that are held to be based on reason.'[13]

The Generic Rights

As the agent must have 'capacity' to do X voluntarily for E, having the 'capacity' of action is crucial for its action. The rights to generic capacities of action, i.e., the 'generic conditions of agency (GCA),' are termed the **'generic rights.'**

Obviously, not every need/ interest/ condition is generic to an agent. The needs of agency are generic only if 'they are prerequisites of an ability to act at all or *with any general* chances of success.'[14] To identify whether a need is generic, the first task is to

[9] Ibid 72.
[10] Gewirth, *Reason and Morality* 26, 171.
[11] Gewirth distinguishes an agent from a prospective purposive performer of actions (PPA). A PPA refers to a being that at least have the capacities required for agency– at least some disposition to exercise them. In this regard, it has capacities or at least some disposition to exercise them to control its performance of doing X through its unforced choice so as to try to achieve E, no matter E is in the action itself or in something to be achieved by the action. It is noted that the idea of PPA has been covered by the scope of 'agent' by Beyleveld and Brownsword. Beyleveld and Brownsword, *Human Dignity in Bioethics and Biolaw* 72.
[12] Deryck Beyleveld and Roger Brownsword, *Consent in the Law* (Hart Publishing 2007) 39.
[13] Gewirth, *Reason and Morality* 171. Gewirth uses the term 'reason' in a very strict sense as comprising only the criteria of deductive and inductive logic. See ibid 22-23.
[14] Beyleveld and Brownsword, *Human Dignity in Bioethics and Biolaw* 70.

be clear on whether agency needs depend on the purpose being pursued. If a need is for a specific purpose and is neither essential nor sufficient to some other general purposes, then this need is not generic. Consequently, for generic needs of agency, the purpose of action is irrespective. This is because it may consist either of the action itself or in an outcome of the action.[15] Due to the presence of the GCA, i.e., voluntariness (or freedom) and purposiveness (intentionality),[16] what matters from the standpoint of the agent is that the purpose, in this motivational sense, *seems* to the agent to be good.[17]

The second stage of identifying the generic needs is to look at whether they are prerequisites of an ability to act at all or with any general chance of success. For those generic needs of an ability to act at all, they are more necessary than those with any general chances of success. The generic needs of agency are, hence, *hierarchical*.[18] Since the generic needs of agency are ordered hierarchically, it is possible for one need to override another *when there is a conflict*. In this respect, logically, only a generic need of agency can outrank another generic need of agency.

From the standpoint of the rational agent, Gewirth indicates that three kinds of generic needs are included, whatever the purpose being purposed. First, Gewirth regards the generic needs of an ability to act at all, i.e., 'the general necessary preconditions of action,' as '**basic needs (goods)**.'[19] The scope of basic needs encompasses physical and psychological dispositions such as life itself, capacities involved in an ability to make choices, and possession of mental equilibrium

[15] Gewirth, *Reason and Morality* 27.
[16] This is only under a general situation, for some exceptions such as purposiveness in the achieve-mental mode. See ibid 62.
[17] Ibid 51-52.
[18] Ibid 63.
[19] Ibid 54.

sufficient to enable one to achieve their purpose for very possibility.[20] To interfere with the basic need, therefore, is to either destroy the prerequisites of the ability to act, or to diminish the chances of the agent to act at all.

The other two categories of needs fall within the scope of the abilities for the possibility of successful action. These two kinds of needs, which are constitutive of an agent's purpose, include so-called '**non-subtractive needs**' and '**additive needs**.' Non-subtractive needs consist of an agent's 'retaining and not losing whatever he already has that he regards as good.'[21] To diminish non-subtractive needs, i.e., the goods that an agent already has for successful actions, is to diminish the chance of achieving its purposes. On the other hand, additive needs consist of an agent's required needs and conditions in order to improve its capacity for successful action. Instead of preventing the loss of something that an agent has already acquired, additive goods are something it intends to gain.[22]

3.3 The Dialectically Necessary Argument to the PGC

3.3.1 The Dialectically Necessary Argument

Gewirth terms his argument *to*[23] the PGC a 'dialectically necessary' method to justify the PGC.[24] Firstly his method proceeds from the standpoint of the agent – in a form of an internal dialogue, which is claimed by using a first-person perspective. His

[20] Ibid.
[21] Ibid 54-55.
[22] It should be noted that, to be clear, according to Gewirth, additive goods are not basic or non-subtractive. Ibid 56.
[23] As Beyleveld puts, this argument is an argument *to* the PGC rather than an argument *from* the PGC. The latter one means a specific issue that the PGC is applied to. Beyleveld, 'Legal Theory and Dialectically Contingent Justifications for the Principle of Generic Consistency' 15.
[24] Gewirth, *Reason and Morality* 44. Also, Deryck Beyleveld and Roger Brownsword, *Law as a Moral Judgement* (Sweet and Maxwell 1986) 129.

argument is thus dialectical; secondly, the formulated argument is dialectically necessary because it follows *logically* from a premise that no agent can coherently deny that it is an agent. This argument is presented to support the assertion that the PGC is the supreme principle of all ethics and law (including bioethics and biolaw) in so far as these are concerned with prescriptions.[25]

The *dialectically necessary justification* can be outlined in three stages. By claiming to be an agent, I, by definition, must claim that:

Stage I

1. **I do something (X) voluntarily for a purpose (E) that I have freely chosen.** Since this purpose was freely chosen, I attach sufficient value to this purpose to motivate me to pursue it; thus, it is *dialectically necessary* to accept.

2. **My (freely chosen) purpose (E) is good** (in this motivational sense). Besides,

3. **There are generic needs of agency**. The needs of agency are generic if they are prerequisites of an ability to act at all or with any general chances of success, *regardless of the purposes* being pursued. On the basis of *the principle of instrumental reason*, whoever (insofar as this agent acts rationally) values/ pursues/ defends E, ought to value/ pursue/ defend the necessary means to E, whatever E might be. Since I must follow the principle that 'whoever pursues an end must be prepared to pursue the means necessary to achieve the end' (because being an agent, by definition, I do things as perceived means to my chosen ends), therefore, I must accept:

4. **My having the generic needs is good for my achieving my purpose**

[25] Beyleveld and Brownsword, *Human Dignity in Bioethics and Biolaw* 69.

(E), *whatever my purpose might be*. Also, it is equivalent to saying that **my having the generic needs is categorically instrumentally good for me**. Because I value my pursued purposes proactively, I must accept:

Stage II

5. I categorically instrumentally ought to pursue my having the generic needs in order to pursue my purposes. Because the agent must value the generic needs only instrumentally, the agent cannot be prohibited categorically from waiving the benefits that having the generic needs would confer, therefore, I must accept:

6. Other agents categorically ought not to interfere with my having the generic needs against *my will*, and ought to aid me to secure the generic needs when I cannot do so by my own unaided efforts *if I so wish*, which means, I must accept that:

7. I have both negative and positive claim rights to have the generic conditions of agency. In short, **I must accept that: I have the generic rights**. It follows purely logically (**Argument from the Sufficiency of Agency, ASA,** which will be presented below) that I must hold that **I am an agent → I have the generic rights** at the same time.

Stage III

8. It follows by the logical principle of universalisability (**LPU**, stated

below) that I must accept that **an agent has the generic rights,** and hence, by the conjunction of steps 7 and 8, I must accept:

9. All agents have the generic rights. Again, on the basis of the LPU, therefore,

10. It is dialectically necessary *for every* agent to accept that *all* agents have the generic rights. In other words,

11. Agents must accept that in their actions they must consider and take into account all agents' claims to have both their negative and positive rights to have the generic rights, namely, that they are agents. Therefore,

12. Agents must act in accordance with the generic rights of all agents, which is what the PGC requires.

Two ideas set out above need to be explained: the **ASA** and the **LPU**. First, the ASA can be described as follows:

7.1 To deny that '**I am an agent → I have the generic rights**' is to deny that the fact that '**I am an agent is sufficient for me to have the generic rights**', which is logically equivalent to asserting that

7.2 It is necessary to satisfy **condition** (or, property)[26] **D** in order for me to have the generic rights. This condition D is not necessarily connected with my being an agent i.e. some agents might have D, some might lack D. In other words, I affirm that '**I have the generic rights → I have D**'. Therefore,

[26] The possession of a 'property' D has been addressed in early contributions of Beyleveld and Brownsword, e.g., ibid 75, Beyleveld, 'Legal Theory and Dialectically Contingent Justifications for the Principle of Generic Consistency' 22-23. It has been changed to satisfaction of a 'condition' in Deryck Beyleveld and Gerhard Bos, 'The Foundational Role of the Principle of Instrumental Reason in Gerwirth's Argument for the Principle of Generic Consistency: A Response to Andrew Chitty' (2009) 20 King's Law Journal 7-8. The authors of the latest contribution note that it does not influence the whole structure and validity of the ASA.

7.3 I assert that without satisfying condition **D**, I do not have the generic rights – although I am an agent.

7.4 However, according to the establishment of 7, **I must accept that I have the generic rights,** which means I am an agent (by definition) and *at the same time* I have the generic rights. In other words, it *cannot* be the case that I contradict that I am an agent if I do not consider that I have the generic rights.

7.5 Therefore, if I assert by holding 7.3 is for me to contradict that I am an agent. Since I am an agent by definition, I must *deny* 7.3, and hence deny its equivalent 7.2. Hence, affirming that **I am an agent is sufficient for me to have the generic rights**.

7.6 Thus, because I must affirm that **I am an agent, this is sufficient for me to have the generic rights**, as it demonstrates that '**I am an agent → I have the generic rights**'.

Secondly, the **LPU** may be stated as follows.

8.1 If **S** is a system of reasoning in which '**S_1 has the property Q, which is sufficient for S_1 to have the property P**' is valid, then '**S_2 has the property Q, which is sufficient for S_2 to have the property P**' is also a valid inference in **S**.[27]

This pure logical principle is applied by Gewirth in order to show that 'whatever is right for one person must be right for any similar person in similar circumstances.'[28]

[27] Beyleveld, 'Legal Theory and Dialectically Contingent Justifications for the Principle of Generic Consistency' 21. See also: Gewirth, *Reason and Morality* 105-107.
[28] Gewirth, *Reason and Morality* 105.

3.3.2 Objections and Replies

This subsection aims to present some major criticisms and their replies of Gewirth's argument to the PGC. As we shall see, most of sceptics focus on stages II and III.[29]

Objections and Replies to Stage I

Sherline argues that **step 4** of the argument fails.[30] This is because, he claims, the argument relies on the principle of hypothetical imperatives which is neither logical nor analytic. He contends that, on the basis of the fundamental concept of this principle, what an agent is required to accept is not something that an agent is logically required to accept. This is to say that if an agent refused to accept the requirement, he/ she/ it would not contradict that he/ she/ it is an agent. However, it has been noted that Sherline fails to realise that an agent, according to the definition, who did not accept this principle would not be able to act, and, consequently, would not be an agent.[31]

Objections and Replies to Stage II

Williams accepts the statement of the '**self-referring ought**.'[32] However, he argues that, from my (the agent's) standpoint of view, the interference from the statement of

[29] Beyleveld and Bos, 'The Foundational Role of the Principle of Instrumental Reason in Gerwirth's Argument for the Principle of Generic Consistency: A Response to Andrew Chitty'20. Also, Beyleveld, 'The Principle of Generic Consistency as the Supreme Principle of Human Rights'6.
[30] Edward D. Sherline, 'Review of The Dialectical Necessity of Morality, by Deryck Beyleveld' (1994) 13 Canadian Philosophical Reviews 75-77.
[31] Beyleveld, 'Legal Theory and Dialectically Contingent Justifications for the Principle of Generic Consistency' 20.
[32] The statement of 'self-referring ought' means that 'I ought to defend/ pursue my possession of the GCA.'

the 'self-referring ought,' to the '**other-referring ought**'[33] relies on a presumption that to deny that 'I have a claim right to the GCA' is to grant the other agent a right to interfere with my GCA.[34] However, this presumption, in his opinion, is false because it contradicts the claim of the 'self-referring ought.'

The denial of statement of the 'other-referring ought,' i.e., 'other agents ought not to interfere with my having GCA', nevertheless, may be *egoistically* considered by that 'it is neither permissible nor impermissible for the other agent to interfere with my GCA,' which does not require me to permit the other agent to interfere with my GCA.[35] In this respect, he contends that[36]

> I can also ask why, if I am going to prescribe that much, I should not more ambitiously prescribe that no one interfere with whatever particular purposes I may happen to have. I want the success of my particular projects, of course, as much as anything else, and I want other people not to interfere with them. Indeed, my need for basic freedom was itself derived from that kind of want. But the argument is certainly not going to allow me to prescribe for all my particular wants.

This is, indeed, a weak claim against the argument.[37] However, this denial is not consistent with the acceptance of the statement of the '**self-referring ought**' (which is also accepted by Williams). As the assertion that 'I ought to defend/ pursue my possession of the GCA' is **dialectically necessary**, I am required to assent to the claim that I must have a negative attitude toward any interference with my GCA. In this

---

[33] The statement of 'other-referring ought' means that 'I have a claim right to the GCA.'
[34] Deryck Beyleveld, *The Dialectical Necessity of Morality: An Analysis and Defence of Alan Gewirth's Argument to the Principle of Generic Consistency* (The University of Chicago Press 1991) 166-171.
[35] Bernard Williams, *Ethics and the Limits of Philosophy* (Taylor & Francis 2006) 61.
[36] Indeed, Williams points out that the argument 'depends on a particular conception of the business of making rules, a conception that lies at the heart of the Kantian enterprise.' Ibid 62.
[37] Beyleveld, *The Dialectical Necessity of Morality: An Analysis and Defence of Alan Gewirth's Argument to the Principle of Generic Consistency* 371.

regard, the suggested interpretation of the denial of the claim that I have a right to my GCA is compatible with my not having a negative attitude towards such interference. Accordingly, the above interference from 'I ought to defend/ pursue my possession of the GCA' to 'I have a claim right to the GCA' does not rely on 'an unjustifiably limited interpretation of the denial' of the later claim.[38]

Moreover, Sherline argues that **step 5** of the argument raises a question concerning the use of principle that 'ought' implies 'can.'[39] He claims that it is neither logical nor analytical. Moreover, it might not be even, as he states, moral. However, the argument uses the principle that 'it is correlative to the principle of hypothetical imperatives,' and an agent 'is required to assent to its requirements for the same reasons.'[40] Hence, this objection is invalid.

Objections and Replies to Stage III

Without seriously taking account the presentation of the ASA involved in effecting **steps 7 and 8**, a variety of objections can be put forth with respect to these two steps (thus Stages II and III are both involved).[41] For example, Bond claims that, as the generic rights are prudential rights secured according to my advocacy of my own

[38] Ibid 371.
[39] Sherline (n 30) 75-77.
[40] Beyleveld, 'Legal Theory and Dialectically Contingent Justifications for the Principle of Generic Consistency' 20.
[41] E.g., Adina Schwartz, 'Review of Reason and Morality, by Alan Gewirth' (1979) 88 Philosophical Review 654-656, EJ Bond, 'Gewirth on Reason and Morality' (1980) 11 Metaphilosopy 36-53, RB Brandt, 'The Future of Ethics' (1981) 15 Nous31-40, Gilbert Harman, 'Justice and Moral Bargaining' (1983) 1 Social Philosophy and Policy114-131, Richard M. Hare, 'Do Agents Have to Be Moralists?' in Jr. Edward Regis (ed), *Gewirth's Ethical Rationalism: Critical Essays with a Reply by Alan Gewirth* (University of Chicago Press 1984) 52-58, Christopher McMahon, 'Gewirth's Justification of Morality' (1986) 50 Philosophical Studies261-281, James P. Sterba, 'Justifying Morality: The Right and the Wrong Ways' (1987) 72 Synthese 45-69. For a detailed reply to objections in relation to prudential / moral rights claim issues about stage III of the dialectically necessary argument, see discussions with respect to objection #47 in Beyleveld, *The Dialectical Necessity of Morality: An Analysis and Defence of Alan Gewirth's Argument to the Principle of Generic Consistency* 257-281.

interests, any universalised rights must be also prudential.[42] It is thus contended by Bond that the argument of 'I must consider that an agent has a right to its GCA by application of the LPU' cannot be established 'without supposing that the rights-claim of Stage II is a moral right.'[43] Similarly, Brandt claims that because the generic rights are secured according to the criterion of my agency interests and rights, universalization can only show that other agents must consider that they have generic rights as well.[44] Moreover, other agents must also consider that any attempt to show that it follows that agents must respect each other's generic rights claims requires a supposition that agents necessarily value the interests of others.[45]

However, it must be noted that the LPU can be internally applied, which shows that the LPU is applied to the inference that is dialectically necessary within my internal viewpoint as an agent, making the claim 'an agent who has a categorical need for generic conditions of agency has a claim right to generic conditions of agency' dialectically necessary within my internal viewpoint as an agent.[46] In response to Bond's objection, therefore, Beyleveld points out that he fails to consider the *internal application* of the LPU.[47]

The ASA makes the application of the LPU straightforward and proves that it is dialectically necessary for an agent to recognise that other agents have the generic rights.[48] This argument, however, has also been criticised. For example,[49] considering

---

[42] Bond (n 41) 50-51.
[43] Beyleveld, *The Dialectical Necessity of Morality: An Analysis and Defence of Alan Gewirth's Argument to the Principle of Generic Consistency* 259-261.
[44] Brandt (n 41) 31, 39-40.
[45] The reply offered by Beyleveld can be found at: Beyleveld, *The Dialectical Necessity of Morality: An Analysis and Defence of Alan Gewirth's Argument to the Principle of Generic Consistency* 464-465.
[46] On the other hand, the external application of the LPU means that the LPU is applied from a dialectically necessary inference within my internal standpoint that all agents must consider the fact that they categorically need their generic conditions of agency give them a claim right to their generic conditions of agency. Ibid 59.
[47] Ibid 261.
[48] Indeed, with respect to stage III of the dialectically necessary argument, Williams notes that 'It rests

the question of whether any agent can be substituted in my dialectical reasoning, suppose there are:

> Claim $\mathbf{C_1}$: possession of one specific instance of condition D will only belong to the agent from whose viewpoint the argument is conducted, i.e., 'I am a member of the class of beings that necessarily values *my* purpose;' and
>
> Claim $\mathbf{C_2}$: possession of D defining agents as a class will be possessed by *all agents*, i.e., 'I am a member of the class of beings that necessarily values *their own* purpose;

Scheuermann claims that the ASA can only show that the agent must take $\mathbf{C_1}$, rather than $\mathbf{C_2}$, to be the sufficient reason for her/ his/ its claim to have the generic rights.[50] This implies an assumption that, without any justification, any agent can be substituted in my dialectical reasoning.

However, it is indicated by Beyleveld that this assumption is not necessary.[51] This is because $\mathbf{C_1}$ implies $\mathbf{C_2}$, and conversely, $\mathbf{C_2}$ implies $\mathbf{C_1}$: these two claims mutually support each other. Accordingly, 'they are substitutable in the argument at

---

on the weakest and least contestable version of a "principle of universalizability," which is brought into play simply by because or in virtue of. If a particular consideration is really enough to establish a conclusion in my case, then it is enough to establish it in anyone's case. That must be so if enough is indeed enough.' Williams (n 35) 60.

[49] For one of the other few objections in terms of the validity of the ASA, see: Singer 177-195. In his reply, Beyleveld contends that although there is an error in holding the principle of $[(P \,\&\, Q) \rightarrow R] \rightarrow [P \rightarrow (Q \rightarrow R)]$ holds in entailment when defending the ASA in his work, 'it does not actually require this principle to hold in entailment.' See: Beyleveld, 'A Reply to Marcus G. Singer on Gewirth, Beyleveld and Dialectical Necessity' 458-473.

[50] James Scheuermann, 'Gewirth's Concept of Prudential Rights' (1987) 37 Philosophical Quarterly 291-304.

[51] Beyleveld, *The Dialectical Necessity of Morality: An Analysis and Defence of Alan Gewirth's Argument to the Principle of Generic Consistency* 288-300. Also, Pattinson (n 3) 10-11.

any point where prediction of agency is the only issue.'[52]

Noticing the involvement of the ASA in effecting **Steps 7 and 8**, furthermore, Chitty argues that Stage III remains invalid.[53] He accepts that, on the grounds that I need the GCA to act for any of my purpose E and the principle of instrumental reasoning, I have the rights to the GCA. However, he argues that step 8 does not follow step 7. This is because step 8 can only follow step 7 if the former steps can be generalised to an argument showing that 'I had to conclude that *any* agent had generic rights.' Nevertheless, such a generalised argument cannot be valid. This is because, as Chitty argues, in steps 1-7, even if it is accepted that any agent has to accept that herself/ himself/ itself has generic rights, *the protagonist and the subject would still be the same person*. Hence, the validity of the argument from step 1 to step 7 depends on the fact that its protagonist is the same person as its subject. Accordingly, step 7 cannot be generalised to step 8, as it only works for the case in which its subject is the protagonist of the argument.

In his reply, Beyleveld contends that although Chitty seems to accept that I have the rights to the GCA (in what we have seen in Stage I of the argument), he does not take at least two crucial points into consideration:

C_a: I contradict that I am an agent *per se* if I do not evaluate actions in terms of my prudential criterion; and

C_b: The principle of instrumental reason: If my doing/ having X is necessary to achieve my purpose E, I ought to attach the same proactive value to my

[52] Beyleveld and Bos, 'The Foundational Role of the Principle of Instrumental Reason in Gerwirth's Argument for the Principle of Generic Consistency: A Response to Andrew Chitty' 12.
[53] Andrew Chitty, 'Protagonist and Subject in Gewirth's Argument for Human Rights' (2008) 19 King's Law Journal 1-26.

doing/ having X as I attach to E.

In this regard, on the basis of the acceptance of claim $\mathbf{C_a}$, I am only rationally compelled to consider that I have the rights that are formally validated by my prudential criterion. Crucially, it should be noted that '[t]he epistemological status of my rights claim is then neither *merely* nor *essentially* prudential, but (for me) *also* and essentially dialectically necessary.'[54] In combination of the acceptance of claim $\mathbf{C_b}$, because the rational requirement for me to evaluate actions in terms of my prudential criterion is a function of $\mathbf{C_b}$, 'the dialectically necessity for me to accept what is validated relative to my prudential criterion, and with it the validity of Gewirth's argument as a whole, rests on it being dialectically necessary for me to employ the principle of instrumental reason.'[55]

Overall, two main types of sceptics can be identified. First, as Williams contends, interference from the 'self-referring ought' to 'other-referring ought' relied on a 'false' presumption. Secondly, there are doubts on the ASA and applications of the LPU. Although objections to this argument are continuously being made, the identification of the flaw is yet to be successfully reached. Indeed, even if there is a flaw in stages II and III, the alternative argument set out below is capable of dealing with this.

3.4 An Alternative Argument: The Dialectically Contingent Argument form the Acceptance of Human Rights

An alternative argument to the PGC is presented by Beyleveld in his contribution *The*

[54] Beyleveld and Bos, 'The Foundational Role of the Principle of Instrumental Reason in Gerwirth's Argument for the Principle of Generic Consistency: A Response to Andrew Chitty' 3.
[55] Ibid 3.

Principle of Generic Consistency as the Supreme Principle of Human Rights.[56]

As we have seen, stages II and III of the dialectically necessary argument have been criticised by most sceptics. In this regard, in combination with the dialectically necessary argument and the dialectically contingent argument, it is put forth by Beyleveld that:[57]

Stage I

1. **Suppose that stage I of the dialectically necessary argument**, i.e., the claim that 'my having the GCA is categorically instrumentally good for me,' **is valid**; and that
2. **I, as a matter of contingent fact, make the impartial assumption that I am committed to treat any other agent's need for the GCA with the same concern and respect as I treat my own**. I consider that any others' need for the GCA must be treated as though their need were my own, in determining what I may do.
3. Running the risk of contradicting this impartiality, or denying that I am an agent, I must hold that unless any other agent is willing to accept generic harms, I categorically ought to act in any other agent's generic needs. This entails that **I categorically ought to act in any other agent's generic needs, in accordance with her/ his/ its will.** This entails that
4. **Any other agent has the generic rights.** It follows that on pain of denying: (1)

[56] Beyleveld, 'The Principle of Generic Consistency as the Supreme Principle of Human Rights'1-18. This version of dialectically contingent argument for the PGC has been regarded as a version of 'the argument form categorically binding other-regarding categorically obligatory requirements on action,' or 'the argument from morality.' Ibid 16. It is noted that a morality, under the PGC, is a set of other-regarding (i.e., addressing at least in part to every agent and concerning with furthering the interests) thesis. For the dialectically contingent arguments to the PGC, see: Beyleveld, 'Legal Theory and Dialectically Contingent Justifications for the Principle of Generic Consistency' 15-41. Beyleveld and Brownsword, *Human Dignity in Bioethics and Biolaw* 77-82.

[57] Beyleveld, 'The Principle of Generic Consistency as the Supreme Principle of Human Rights' 6-8.

that all agents categorically ought to be treated completely equally; or (2) that as I am an agent, **I must accept that all agents,** including me and any other agent (other than me), **have the generic rights.** This entails that:

5. **All permissible actions must be consistent with the generic rights of all agents**, which is what the PGC requires.

Stage II

6. The idea that '**everyone should be treated equally**' is a widely accepted premise, stated in human rights instruments as an initial and universal value[58] and confirmed by the courts continuously and consistently.[59] Taking for example the Preamble[60] and Articles 1[61] and 2[62] of the UDHR, since international human rights conventions generally claim that all human beings are equal in dignity and rights, it entails that all human agents categorically ought to be treated as equal in dignity and rights. **Accordingly, human rights treaties/ provisions commit to complete impartiality** of this alternative argument on pain of denying that the Declaration can have any coherent

[58] It is argued that the ideas of liberty, equality and fraternity are followed by very first human rights instruments. Beyleveld and Brownsword, *Human Dignity in Bioethics and Biolaw* 80. Moreover, the idea of 'everyone should be treated equal' is equivalent to saying that each person is to have equal right to a community. The latter idea is in line with the first principle of justice of Rawlsian theory of justice. See discussions below.

[59] Most of philosophical arguments for competing moral principles are demonstrated according to contingencies of this idea. Beyleveld and Brownsword, *Consent in the Law* 44. For example, as Rawls puts, in 'the most extensive total system of equal basic liberties compatible with a similar system for all.' John Rawls, *A Theory of Justice* (Revised edn, Belknap Press of Harvard University Press 1999) 206-207.

[60] The very first sentence of the Preamble of the UDHR declares that it recognises 'the inherent dignity and of the equal and inalienable rights of all members of the human family is the foundation of freedom, justice and peace in the world.'

[61] Article 1 puts that 'All human beings are born free and equal in dignity and right. They are endowed with reason and conscience and should act towards one another in a spirit of brotherhood.'

[62] Article 2 states that 'Everyone is entitled to all the rights and freedoms set forth in this Declaration, without distinction of any kind…'

application to or by human agents.

7. This does not, however, necessarily follow that the human rights instruments/ conventions, e.g., the UDHR, are committed to the PGC. This is because the impartiality required by the PGC operates between agents towards the GCA, whereas the impartiality stated in the human rights instruments operates between humans towards rights enshrined in the conventions. To show that human rights instruments are committed to the PGC, **it must be declared that the existence of any human rights implies declaring that human agents have human rights to the generic rights, or justifying that it is dialectically necessary for me to have claim rights to the GCA.** However, as the approach of the alternative argument is to 'skip' stages II and III of the dialectically necessary argument, thus constituting a rejection of all scepticism about these two stages, the latter argument is not considered here (although it is valid).
8. The GCA are needed to be able to exercise any right to act.[63] On the basis of the principle of instrumental reason (as in stage I of the dialectically necessary argument), it is insincere to claim that an agent has a human right to do something without granting this agent a right to possess the means necessary for it to exercise that right. Accordingly, **appreciation of the concept of the GCA requires those who accept the human rights conventions to hold that human agents have human rights to the GCA**.
9. Again, however, it should be emphasised that **only the acceptance of human rights that satisfy all features of generic rights result in the recognition**

[63] This implies that the scope of rights protected by the UDHR or any other human rights instruments can be wider than human rights to the GCA. Indeed, the PGC welcomes human rights other than the generic rights. The only thing matter is that the GCA are needed to be able to realise the declared human rights.

that the PGC is a necessary criterion of legal validity. Therefore, any human rights instruments under the will-conception must, 'on pain of contradicting that it is a convention on human rights, be interpreted in line with the requirements of the PGC.'[64]

10. Nevertheless, since the rights to the GCA are assumed to be compatible with the conclusion of stage I of the dialectically necessary argument, **the rights to the GCA implied by the human rights instruments must be assigned as rights under the will conception**.
11. Accordingly, **the recognition of the impartiality of human rights instruments with respect to dignity and inalienable rights entails acceptance of the rights granted by the PGC**.

The alternative argument considers the implications of stage I of the dialectically necessary argument for the interpretation of human rights.[65] Structurally, stage I of it presents the methodology of the alternative argument: if the first stage of the dialectically necessary argument is sound, and the impartial assumption that human beings are equal in dignity and rights is accepted, the claim that 'all agents should act in accordance with the generic rights of all agents' must follow. The second stage, takes the UDHR, which proclaims its acceptance of the impartiality assumption, as an example, showing that appreciation of the concept of the GCA requires those who accept human rights conventions to hold that human agents have human rights to the GCA.

Since the coupling of categorical necessity of the conclusion of stage I of Gewirth's argument with a commitment to whole impartiality requires me to grant the

[64] Beyleveld and Brownsword, *Human Dignity in Bioethics and Biolaw* 82.
[65] Beyleveld, 'The Principle of Generic Consistency as the Supreme Principle of Human Rights' 6.

generic rights to any other agent, stage II of the dialectically necessary argument is valid. Because I have the same attitude towards any other agent's need for the GCA as I must have toward my own need for the GCA (on the basis of the requirement of the complete impartiality assumption), I must grant the generic rights of any other agent.[66] In this respect, the attitude I must have towards my need for the GCA 'must be equivalent in meaning to or entail' that I have claim rights to the GCA.[67] This is not to assume that I am **actually** committed to complete impartiality. Rather, this attitudinal equivalence is 'a direct implication of the fact' that if I were to have the same *normative attitude* towards any other agent's need for the GCA as I must have towards my own need for it, I would be required to grant any other agent the generic rights.[68]

According to this alternative argument, it is supposed that stage I of the dialectically necessary argument is sound. However, in this regard, this argument 'implies that the only possible problem with the dialectical necessary argument lies with stage III.'[69] Nevertheless, as illustrated in the last section, these objections are not convincing.

However, there are limitations to this alternative argument. The most obvious one is that this argument does not fully render the PGC dialectically necessary, as the premise that 'every human being categorically ought to be treated equally' is a dialectically contingent premise. Hence, the argument does not present that this contingent premise *must* be accepted.[70] It thus seems that the premise is based on external considerations. Nevertheless, it is arguable that this contingent line of

[66] Ibid 7-8.
[67] Ibid 8.
[68] Ibid 8.
[69] Ibid 8.
[70] Ibid 16-17.

reasoning is commonly accepted by different individuals and cultures[71] – at least, this is accepted in the European and Formosan legal regime. Moreover, there are, indeed, claims that this contingent premise is valid. For example, Gauthier argues that, although not necessarily in all cases, it is in our interest to treat everyone equally in general (as we are not perfect).[72]

If these arguments are sound, then 'any legal system that recognizes human rights (under the requisite conception of these) must regard actions that violate human rights as legally invalid.'[73] Therefore, the enforcement machinery of any part of a network of international human rights treaties of universal or regional application, e.g., the ICCPR, the ICESCR, the ECHR[74] and the European Union Charter of Fundamental Rights, must be interpreted to conform to the PGC.[75]

3.5 The Content of Agency Rights

A handful of features of the generic rights, which are interpretive and justificatory consequences of the dialectically necessary argument as well as the entailment of the alternative justification set out in the last section, must be noted.[76] First, the dialectically necessary argument for the PGC renders it dialectically necessary for

[71] Ibid 17.
[72] David Gauthier, *Morals by Agreement* (OUP 1986), citing from Beyleveld, 'The Principle of Generic Consistency as the Supreme Principle of Human Rights' 17.
[73] Beyleveld and Brownsword, *Human Dignity in Bioethics and Biolaw* 69.
[74] It is arguable that the fundamental rights and freedoms grants by the ECHR can be viewed as rights to capacities (or other features) that are necessary to exercise of any rights at all. If this argument is valid, the rights claimed by the ECHR correspond to the generic conditions of agency. Deryck Beyleveld, 'Data Protection and Genetics: Medical Research and the Public Good' (2007) 18 King's Law Journal 286.
[75] In fact, Beyleveld and Brownsword argue that the human rights instruments 'do operate with' the features of human rights required above. See: Beyleveld and Brownsword, *Human Dignity in Bioethics and Biolaw* 82.
[76] Beyleveld, 'The Principle of Generic Consistency as the Supreme Principle of Human Rights' 8-16.

agents to grant **inalienable** generic rights to **all agents**. The PGC thus imposes duties on other agents to respect the generic needs of an agent, no matter whether those generic rights are **positive or negative**.

Secondly, the PGC is a moral[77] principle and the generic rights are rights under the **will conception** of rights.[78] The will-conception of rights means that an agent has no perfect duty to itself to defend its possession of these generic conditions. In this respect, agents can waive the benefits of the GCA. This is different from the interest conception of rights holding that agents accept a perfect duty to themselves, as this conception of rights argues that the primary function of human rights is to protect and promote certain essential human *interests*. [79] In this regard, the generic rights are claim-rights under the will-conception means that 'duties imposed on other agents by the positive rights are subject to the rights-holder wishing assistance, while duties imposed by negative rights are subject to interference being against the rights-holder's will.'[80]

With respect to these features, a question immediately and inevitably comes to mind: as the dialectically necessary argument grants the generic rights per se to all agents, then, can other beings, such as those beings with only *part* of the capacities to control their performance of doing X through their unforced choice so as try to achieve E, whatever E is, possess quasi-generic rights?

Gewirth states his argument of extending the objects of the generic rights from

[77] According to Gewirth's theory, '[a] morality is a set of categorically obligatory requirements for action that are addressed at least in part to every actual or prospective agent, and that are concerned with furthering the interests, especially the most important interests, of persons or recipients other than or in addition to the agent or the speaker.' Gewirth, *Reason and Morality* 1.
[78] Beyleveld and Brownsword, *Human Dignity in Bioethics and Biolaw* 71-72.
[79] In their contribution Beyleveld and Brownsword reject Gewirth's argument that there are ways in which agents can have perfect duties to themselves. Ibid 106-108. Gewirth, *Reason and Morality* 334.
[80] Deryck Beyleveld and Shaun D. Pattinson, 'Moral Interests, Privacy, and Medical Research' in Michael Boylan (ed), *International Public Health Policy and Ethics* (Springer Netherlands 2008) 2.

agents to *partial* agents as follows:[81]

1. Being an agent is only necessary to possess *full* generic rights. This is because the ASA of the dialectically necessary argument demonstrates that being an agent **is sufficient for it to possess ALL generic rights**.[82] Being an agent, hence, is sufficient, but not necessary for possessing generic rights. The PGC thus grants moral status to non-agents.
2. Gewirth applies the principle of proportionality to extend the possession of generic rights to partial agents.[83] He argues that by applying the principle of proportionality, together with the PGC, partial agents possess limited generic rights to a lesser extent. The degree to which partial agents possess generic rights depends upon the degree of approach to agency, i.e., the generic capacity of agency, on a proportional basis.

However, this argument meets objections that suggest that this is not necessarily true: it is argued that having *full* generic capacities of agency is not only necessary and sufficient to possess generic rights in full, but also 'necessary to possess *any generic rights at all*.'[84] This is because:

1. The generic rights are rights under the will-conception of rights. *Only* agents can voluntarily waive the benefits by their free choice when not interfering with their duties to other agents.
2. The PGC reciprocally imposes duties on other agents to respect the generic needs of any other agent, whether the generic rights are positive or negative.

[81] Gewirth, *Reason and Morality* 120-121.
[82] See Section 3.3.1. Also, Beyleveld and Brownsword, *Human Dignity in Bioethics and Biolaw* 118.
[83] Gewirth, *Reason and Morality* 121.
[84] Deryck Beyleveld and Shaun D. Pattinson, 'Precautionary Reasoning as a Link to Moral Action' in Boylan Michael (ed), *Medical Ethics* (Prentice-Hall 2000) 39-53. See also: Beyleveld and Brownsword, *Human Dignity in Bioethics and Biolaw* 118, and Pattinson (n 3) 20-21.

Therefore, *only* agents can be subjects of duties to any degree.

3. The principle of proportionality can *only* be applied to interferences that alter the quantity, *but not the quality*, of holding a property. In this respect, Gewirth's argument commits 'the fallacy of disparateness.'[85] The principle of proportionality cannot therefore derive quasi-generic rights, or at least, cannot be employed to support his 'quasi-generic rights' claim *alone*.
4. Moreover, if Gewirth's claim of quasi-generic rights were valid, then the PGC should require an agent to act in accordance with the generic rights *and* quasi-generic rights of all partial agents. This would add an unnecessary requirement to the PGC and accordingly affect the ontology of his theory.

Therefore, only agents possess *any generic rights at all* and only agents have the duty to respect the generic needs of an agent by the PGC. Nevertheless, this does *not* entail that, when applying the PGC to the real world, agents do not owe generic duties *in relation to* other non-agents. Indeed, the agents also owe the *indirect* duties in relation to those non-agents which have particular relationships/ connections with other agents. To do generic harms to those non-agents is to interfere with the GCA of those agents. For example, if an agent A is a musician who has a piano, since a duty to A is a duty owed as a result of properties (such as this piano) possessed by A, other agents owe duties not to harm the property (piano) of A (apart from the exemptions which can be justified in accordance with the criterion of degrees of needfulness for action).[86]

What about other beings/ creatures without particular relationships/ connections with agents? Beyleveld and Brownsword argue that agents 'must accept that they

[85] Beyleveld and Brownsword, *Human Dignity in Bioethics and Biolaw* 119.
[86] Pattinson (n 3) 4. We shall visit an idea very much similar to this when commenting issues with respect to consent in the data protection principles in section 6.4.1.

have *duties* towards all living creatures (human or non-human) on a proportional basis' by practically approaching the matter from the application of the PGC to beings in the real world and society.[87] In this respect, the first step is to identify which beings are agents in the empirical world.

From the standpoint of an agent, she can *only* ascertain that she is an agent due to her imperfect knowledge towards others. However, according to Beyleveld and Pattinson, the categorical nature of the PGC requires agents to employ precautionary reasoning,[88] which obliges the agents to presume that all 'creatures whose agency is uncertain' are agents.[89] This is because the PGC is a moral principle that is categorically binding. Accordingly, it can never be justified that one ignores any possibility to avoid running the risk of violating the PGC owing to the categorical nature of the PGC. The risk of violating the PGC, therefore, must be minimised in so far as it is possible to do so. For this reason, it is unacceptable to presume that an ostensible agent[90] is not a generic-rights-holder because an agent cannot firmly ascertain that this ostensibly agent is *not* an agent.

Let me explain this through an example. If A is not an agent, to presume that A is an agent can only restrict my act (toward A) to some extent; I am still a holder of generic rights – this does not violate the PGC. On the other hand, however, if I mistakenly presume that A is not an agent, my denial of A's agency, which denies that A is a holder of generic rights, violates the PGC.[91] This mistake can be avoided by

[87] Beyleveld and Brownsword, *Human Dignity in Bioethics and Biolaw* 112.
[88] Beyleveld and Pattinson, 'Precautionary Reasoning as a Link to Moral Action' 39-53.
[89] Pattinson 22-26. Beyleveld and Brownsword, *Human Dignity in Bioethics and Biolaw* 112-113, 121-134.
[90] An ostensible agent is some other being displaying all the characteristics and behaviour expected of an agent. However, as I cannot access this ostensible agent's mind, it is logically possible to say that this ostensible agent is 'merely a cleverly programmed automation without a mind.' Pattinson 22-23.
[91] Beyleveld and Brownsword, *Human Dignity in Bioethics and Biolaw* 121.

employing the precautionary principle suggested by Beyleveld and Pattinson:[92]

> If there is no way of knowing whether or not X has property P, then, is so far as it is possibly to do so, X must be assumed to have Property of P is the consequence of erring in presuming that X does not have P are worse than those of erring in presuming that X has P (and X must be assumed not to have P if the consequences of erring in presuming that X has P are worse than those of assuming that X does not have P.)[93]

Therefore, if A is an ostensible agent, the possibility that A is an agent must be taken to in its entirety.[94]

In the light of the purpose of thesis, I will only discuss privacy and data protection issues in relation to human beings. In this respect, all living human beings at least can be considered as partial ostensible agents.[95] In sum,

A. An agent possesses *any generic rights at all*. Reciprocally, an agent owes duties to respect (act in accordance with) the generic rights of all agents.
B. An agent also owes the *indirect* generic duties *in relation to* those non-agents which have particular relationships / connections with other agents.
C. An agent owes *direct* duties to *all* living creatures (human or non-human

---

[92] Beyleveld and Pattinson, 'Precautionary Reasoning as a Link to Moral Action' 39-53.
[93] Beyleveld and Brownsword, *Human Dignity in Bioethics and Biolaw* 122.
[94] As regards those apparent partial agents who act with a less extent possibility to be agents than ostensible agents, according to '**the criterion of avoidance of more probable harm**,' when these duties to apparent partial agents come into conflict, beings who are more probable agents override less probable agents on a proportional basis. See: ibid 122-123.
[95] As regards those who are apparently no more than partial agents, the PGC still obliges the agents to presume that ALL creatures whose agency are uncertain are agents. This is because the possibility that they are agents cannot be ruled out entirely. With respect to potential agents, it is required by the principle of precautionary to grant some moral status to them according to the strength of evidence they displayed to be potential ostensible agents. This is because, based on the reasoning of precautionary, 'evidence that a being E is a potential ostensible agent is evidence relevant to the possibility that E is an agent.' Ibid 125.

beings whose agency is *uncertain*) on a proportional basis according to the degree of the necessary capacities of agency to which they evidentially act. [96]

The other features of the generic rights will also require a brief discussion.

As the generic rights are granted to agents simply by virtue of being agents, the dialectical necessity of the generic rights renders them inalienable.[97] Furthermore, the generic rights can be positive as well as negative. This is because the fact that the dialectically necessary argument is driven by an agent's categorical instrumental need for the GCA (Stage I). However, this is subject to the proviso that positive action to protect an agent's generic conditions of agency cannot be required of another agent if the other agent's assistance conflicts with (at least) equally important generic rights or interests of another agent.[98]

The understanding that generic rights operate under the will-conception principle entails that an agent can waive the benefits of generic rights if they wish to do so. Accordingly, he/ she/ it does not have duties to protect, or at least not to harm, their own generic agency interests if he/ she/ it does not wish to do so. However, such a waiver should not endanger, again, equally or more important generic rights/ interests of other agents. Moreover, such a waiver should be on the basis of permitting an informed agent to engage freely in activities that are not favourable to the generic agency interests of the agent.[99] As the PGC is dialectically necessary, the dignity of human agents must reside in their capacities for action to achieve the voluntarily chosen purposes. It is therefore contrary to the specific dignity of the agent if the

[96] Stephen Smith, 'Precautionary Reasoning in Determining Moral Worth' in Michael Freeman (ed), *Law and Bioethics: Current Legal Issues Volume 11* (OUP 2008) 204-212.
[97] Beyleveld, 'The Principle of Generic Consistency as the Supreme Principle of Human Rights' 15.
[98] Ibid 14.
[99] Ibid 12.

waiver of the benefits of generic rights is not in accordance with that agent's consent under the right conditions.[100]

I have put forward that whilst considering the waiver of benefits of the generic rights and positive actions to assist an agent if she so wishes, the attention in relation to the hierarchy of generic rights must be considered. In the next section I will present a detailed discussion to illustrate a logical consistency rule which is compatible with a hierarchy whereby some interests/ rights are overridden by others.

3.6 How the PGC Approaches the Question of Reconciling Competing Rights and Interests: the Criterion of Degrees of Needfulness for Action

Essentially from the will-based conception of Gewirthian moral theory, agents are permitted to do anything as long as they are not violating generic rights of other agents. In this case, there are possibilities for conflicts to occur between generic rights of different agents. According to Gewirth, the duty to respect agents having the more necessary goods takes precedence over the duty to respect their having the other goods **when two duties conflict**.[101] Based on the restrictions imposed by the PGC, considerations resolving conflicts of rights are presented in relation to the *direct*[102] application of the PGC:[103]

---

[100] The conditions are unforced and informed choice. Beyleveld and Brownsword, *Consent in the Law* 7.

[101] Gewirth, *Reason and Morality* 340.

[102] For discussion with regard to indirect application of the PGC, see section 4.3.

[103] These rules at some level echo the argument of proportionality under precaution in play. The author already regarded the principle of proportionality and consent issues when delivering the descriptive chapter in relation to the ECHR.

1. To deal with conflicts of rights/ interests of the same degree of importance, one must follow the criterion of prevention or removal of inconsistency, namely, '[i]f one person or group violates or is about to violate the generic rights of another and thereby incurs transactional inconsistency, action to prevent or remove the inconsistency may be justified.'[104]
2. The criterion of degrees of needfulness for action is used to deal with 'goods of the different degree of importance, but mainly within the same general context of preventing transactional inconsistency.'[105] This criterion can be expressed as follows:

(1) The basic needs are the most necessary of all generic needs.

(2) Within the category of the needs for the possibility of successful action, non-subtractive needs are more necessary than additive ones, thus in the case of conflict, rights to non-subtractive needs outweigh rights to additive needs. This is because, as Gewirth points out, possessing the former needs is usually a necessary condition of being able to acquiring the latter needs.[106]

It should be noted that, from the standpoint of an agent, within the same *category* of generic needs, there is still an order of generic needs placed 'in a hierarchy according to the degree to which they are needful for action per se and for successful action generally.'[107] Moreover, Gewirth emphasises that this criterion is concerned with 'preventing violations of rights, not with increasing amounts of goods,' which

[104] Gewirth, *Reason and Morality* 342-343.
[105] Ibid 343.
[106] Ibid.
[107] Beyleveld and Brownsword, *Human Dignity in Bioethics and Biolaw* 85. For example, among these basic needs, there is still a hierarchical ordering. Gewirth points out that among basic needs, life is the first priority, followed by various physical and psychological needs such as food, health and shelter. See: Gewirth, *Reason and Morality* 63. A number of examples can be found at: ibid 341-342.

distinguishes it from the utilitarian idea.[108]

Furthermore, the canon of degrees of needfulness for action can be classified in both a qualitative and quantitative way. The former applies from the viewpoint that generic needs of an ability to act at all are apparently more necessary than those with any general chances of success. On the other hand, the latter applies to the idea concerning the interference with other generic needs. No matter which qualitative categories (either ability to act at all or ability to act with any general chances of success) the generic needs fall under, to interfere with a generic need may have quantitative (either greater or lesser) effects.[109]

3. There must be rules governing agents' interactions in a complex society. 'In the case of procedurally justified rules, their requirements override in particular cases the duty not to coerce one's recipients so long as the latter continue voluntarily to accept the rules.'[110] However, it should be noted that only after the fulfilment of the following conditions, these requirements can override 'the duties to refrain from occurrently coercing or harming these persons':[111]

   A. The requirements are necessary to prevent undeserved coercion and serious harm.
   B. The requirements do not go beyond what is needed for such protection.
   C. The taxational coercions and harms imposed are slight by comparison with the harm they remove. The requirements are imposed by the procedures of the method of *consent*.

[108] Gewirth, *Reason and Morality* 344.
[109] Beyleveld and Brownsword, *Human Dignity in Bioethics and Biolaw* 70-71.
[110] Gewirth, *Reason and Morality* 344.
[111] Ibid 344.

Under these conditions, the proportionality principle operating under precaution is called into play.[112] It should be also noted that the three criteria listed above for resolving conflicts are NOT in any respect mutually exclusive.[113] Moreover, although 'such priorities entail that in certain circumstances the requirements of some moral rules justified by the PGC must be overridden by the requirements of other rules that are also justified by the PGC,'[114] this does not 'remove the categoricalness either of the principle or of its derivate rules.'[115]

With reference to practical applications of how the criterion of degrees of needfulness for action and successful action determines the precedence of a right in competing cases, the requirements of the PGC depend on *particular* circumstances when various competing rights come into conflict. In other words, the rights granted by the PGC depend upon 'contingent circumstances attending the interaction of individuals.'[116] The rights that the PGC grants are not absolute in conflicting cases – except the only possible circumstance suggested by Gewirth himself – the right of innocent persons not to be killed against his will.[117]

3.7 Reasons for the Adoption of the PGC and Replies to the Objections

The identification and weight of the rights and interests evoked by the studies focusing on balancing tests will surely differ from one moral theory to another. To

[112] Beyleveld and Brownsword, *Consent in the Law* 55-56.
[113] Gewirth, *Reason and Morality* 345.
[114] Ibid 339.
[115] Ibid.
[116] Beyleveld and Brownsword, *Human Dignity in Bioethics and Biolaw* 83.
[117] Ibid.

most legal researchers, it saves considerable effort to adopt a theory of 'current trend' in their writing up of works. The Gewirthian moral theory applied by the thesis, however, seems difficult to place within the current trend. In this respect, let us take one of the most popular rationalist ethical theories[118] – *Justice Theory of John Rawls* –[119] as an example to show why the thesis does not choose the popular one.

The very initial idea of Rawls' theory to consider justice is to ask, by conducting a thought experiment, which principles we would choose in an 'original position'[120] of equal share of liberties, behind a 'veil of ignorance'[121] that would prevent one from knowing anything about who in particular one is. His conception of Justice Theory demands:[122]

1. Liberty must be maximised, constraints against such a principle is only subject to necessity of protection of liberty itself;
2. **The First Principle** of justice states that

   'Each person is to have an equal right to the most extensive total system of equal basic liberties compatible with a similar system for all;'[123] and

[118] It is observed, for example, that one cannot discuss the issues, at least in the English speaking world, in relation to justice without mentioning John Rawls. See: Ruth Anna Putnam, 'Why Not a Feminist Theory of Justice?' in Martha Craven Nussbaum and Jonathan Glover (eds), *Women, Culture and Development: A Study of Human Capabilities* (OUP 1995) 303. Also, M.D.A Freeman, *Lloyd's Introduction to Jurisprudence* (8th edn, Sweet & Maxwell 2008) 583. Indeed, the Rawlsian theory is also popular in the Mandarin speaking world currently.

[119] The Rawlsian theory is then reformulated by himself in *Political Liberalism*. See: John Rawls, *Political Liberalism: Expanded Edition* (2nd edn, Columbia University Press 2005).

[120] For the idea of 'original position' and its justification, see: Rawls, *A Theory of Justice* 15-17. It is noted that in Rawls' *Political Liberalism*, the 'original position' is addressed as a 'device of a representation.' See: Rawls, *Political Liberalism: Expanded Edition* 15. Briefly, the idea of original position is to 'set up a fair procedure so that any principles agreed will be just.' Rawls, *A Theory of Justice* 118.

[121] Rawls, *A Theory of Justice* 118-119.

[122] Ibid 206-207. Also, Freeman (n 117) 584.

[123] It is noted that in *Political Liberalism*, 'the most extensive total system' is replaced by 'a fully adequate scheme of equal basic liberties.' Rawls, *Political Liberalism: Expanded Edition* 291.

The Second Principle demands: [124]

'Social and economic inequalities are to be arranged so that they are both:

(a) To the greatest benefit of the least advantaged, consistent with the just savings principle, and
(b) Attached to offices and positions open to all under conditions of fair equality of opportunity.'

In the second principle of justice governing a given society's social and economic institutions, principle of 2(a) has been referred to *the difference principle*, whilst 2(b) is termed *the fair opportunity principle*. Furthermore, Rawls contends that in being a rational person, an individual in the original position should recognise that 'they should consider the priority of these principles' in order to assign weights for adjudicating his or her claims on another.[125] The principles of justice, in this regard, are ranked in a 'lexical order' and 'therefore liberty can be restricted only for the sake of liberty.'[126] This is named 'the first priority rule.'[127] 'The second priority rule,' furthermore, states that

1. 'The second principle of justice is lexically prior to the principle of efficiency and to that of maximizing the sum of advantages;' and
2. 'Fair opportunity is prior to the difference principle.'[128]

---

[124] Also, ibid 291.
[125] Rawls, *A Theory of Justice* 37.
[126] Ibid 207.
[127] Two cases in relation to this principle are provided by Rawls:
(a) A less extensive liberty must strengthen the total system of liberty shared by all;
(b) A less than equal liberty must be acceptable to those with the lesser liberty.
[128] Rawls, *A Theory of Justice* 207. Another two cases are provided by Rawls:
(a) An inequality of opportunity must enhance the opportunities of those with the lesser opportunity;
(b) An excessive rate of saving must on balance mitigate the burden of those bearing this hardship.

In terms of this lexical order, 'the order requires us to satisfy the first principle in the ordering before we can move on to the second, the second before we consider the third, and so on.'[129] The lexical order in relation to the priority of weighing competing liberties against each other, similarly to the criterion of degrees of needfulness for action, can be of essence for the purposes of weighing *when conflict of rights and interests is involved*.[130]

However, Gewirth observes that the lexical order of priority is not[131]

> derived from any of his principles, including his first principle of equal freedom; instead, the specific ordering he presents is based on considerations external to the principles, consisting in presumed reasons or motives persons have for choosing the principles …

He argues,[132] moreover, that the arrangements of the lexical order seem to reflect the preferences of Western liberalism 'rather than providing a rational basis or justification of such liberalism.'[133] Comparatively, the Gewirthian justification to the PGC is based on the dialectically necessary argument, which does not require agents to understand and agree with the line of reasoning since it is logically necessary irrespectively of an agent's capacity to know the justification.[134] This character, which does not apply to the Rawlsian justice theory, however, is particularly important for the thesis to develop guidelines regarding regulations of the two technologies in

---

[129] Ibid 38.
[130] See: Chapter 4.
[131] Gewirth, *Reason and Morality* 341.
[132] There is another objection argued by Gewirth in light of the Rawlsian moral theory, namely the inability to appeal to 'independent rational justification' to justify the theory. See: ibid 19. For a similar evaluation of the PGC against the Rawlsian theory, see: Phil Bielby, *Competence and Vulnerability in Biomedical Research* (Springer 2008) 84-87.
[133] Gewirth, *Reason and Morality* 341.
[134] Beyleveld, *The Dialectical Necessity of Morality: An Analysis and Defence of Alan Gewirth's Argument to the Principle of Generic Consistency* 149-150.

privacy and data protection law regimes.[135]

Returning to the popularity of moral theories, it has been said that the PGC is hardly to be suggested as a popular one in academic circles. Indeed, on first reading of Gewirth's argument to the PGC, reviewers (including some leading scholars) might think that they have found certain flaws in the argument.[136] Academic resistance to Gewirth's theory, therefore, has been solid and continuous.[137] This resistance to the PGC is nevertheless, unsuccessful. Indeed, later readings and responses from those Gewirthian scholars frustratingly reveal most of these flaws to be misunderstandings. Most of the critiques against the justification of the PGC rest on stages II and III of the dialectically necessary argument. To me, at least until now, no objection generates insurmountable difficulties.[138] Moreover, the alternative argument that links the first stage of the dialectically necessary argument with the dialectically contingent justification for the PGC, in this case, is able to answer most of the questions.

Debates over the PGC do not form a sound basis against the PGC. By contrast, these academic discussions in terms of the PGC are even more popular: a series of recent discussions regarding the PGC are published in *Ratio Juris* and *King's Law Journal*.[139] Accordingly, the resistance to the PGC does not affect my willingness to

---

[135] See section 7.1.
[136] See section 3.3.
[137] Discussions, criticisms and responses about the argument to the *PGC* can be found at Beyleveld and Brownsword, *Human Dignity in Bioethics and Biolaw* 77-82, 87-110. See also, Beyleveld, 'Legal Theory and Dialectically Contingent Justifications for the Principle of Generic Consistency' 17-19. Pattinson 8-9. Also, Jr. Edward Regis (ed) *Gewirth's Ethical Rationalism: Critical Essays with a Reply by Alan Gewirth* (University of Chicago Press 1984) and Michael Boylan, *Gewirth: Critical Essays on Action, Rationality, and Community* (Rowman & Littlefield 1999).
[138] For a summary of replies to critics, see: Beyleveld, *The Dialectical Necessity of Morality: An Analysis and Defence of Alan Gewirth's Argument to the Principle of Generic Consistency* 360-396.
[139] See: Tony Ward, 'Two Schools of Legal Idealism: A Positivist Introduction' (2006) 19 Ratio Juris127-140, Deryck Beyleveld and Roger Brownsword, 'Principle, Proceduralism, and Precaution in a Community of Rights' (2006) 19 Ratio Juris 141-168, Robert Alexy, 'Effects of Defects—Action or Argument? Thoughts about Deryck Beyleveld and Roger Brownsword's Law as a Moral Judgment' (2006) 19 Ratio Juris 169-179, Peter Koller, 'The Concept of Law and Its Conceptions' (2006) 19 Ratio Juris 184-186, Massimo La Torre, 'On Two Distinct and Opposing Versions of Natural Law: "Exclusive" versus "Inclusive"' (2006) 19 Ratio Juris 197-200, Stuart Toddington, 'The Moral Truth

rest arguments by accepting the PGC as an adequate theoretical framework. Crucially, it should be noted that, as discussed above, the two justifications provided are applicable, adequate and convincing enough to this thesis.

However, while this thesis contends that the PGC is the most powerful theoretical framework for the purposes of this study, it must be proposed that, to be clear, rather than defending or providing full analysis of this moral theory, the major task of this thesis is only to apply it to produce clear guidelines and principles for legislation in Europe and Taiwan. Furthermore, while it is possible for one to challenge that choosing a similar type of framework to the Rawlsian justice theory to compare with the PGC is too selective and too narrow, it must be emphasised that it is not the purpose of this thesis to take an overall evaluation of the PGC against all of the rest of rationalist ethical theories.[140]

3.8 Summary

This chapter has introduced the theoretical framework which this thesis chooses to apply. The PGC has been briefly illustrated. By showing the justifications of the PGC in sections 3.3 and 3.4, I propose the PGC as the supreme moral principle applicable. These arguments also provide sufficient motivation of employing the PGC in this thesis. Then, I outlined the features of the generic rights. I have shown that the generic

about Discourse Theory' (2006) 19 Ratio Juris 217-229. Bev Clucas, 'The Sheffield School and Discourse Theory: Divergences and Similarities in Legal Idealism/Anti-Positivism' (2006) 19 Ratio Juris 230-244, Robert Alexy, 'On the Concept and the Nature of Law' (2008) 21 Ratio Juris 287, Robert Alexy, 'The Dual Nature of Law' (2010) 23 Ratio Juris 176, Søren Holm and John Coggon, 'A Cautionary Note against "Precautionary Reasoning" in Action Guiding Morality ' (2010) 22 Ratio Juris 295-309, Deryck Beyleveld and Shaun D. Pattinson, 'Defending Moral Precaution as a Solution to the Problem of Other Minds: A Reply to Holm and Coggon' (2010) 23 Ratio Juris 258-273, Chitty (n 53) 1-26, and Beyleveld and Bos, 'The Foundational Role of the Principle of Instrumental Reason in Gerwirth's Argument for the Principle of Generic Consistency: A Response to Andrew Chitty' 1-20.

[140] Also, Bielby (n 131) 87.

rights are: (1) granted by the PGC to all agents; (2) inalienable; (3) rights under the will conception; and (4) rights as positive as negative. Section 3.6 addressed direct application of the PGC as the general methodology. By comparing it with one of the most popular theories, additionally, reasons for the adoption of the PGC were further demonstrated in section 3.7. To answer the research question, specific applications of this moral theory to various issues will be explored in the following chapter.

Chapter 4

The Specific Application of the PGC to the Balancing Test Issues

4.1 Introduction

Building on the Gewirthian framework presented in Chapter 3, this chapter aims to elaborate a specific application of the PGC to the balancing test between privacy and competing rights. This will be undertaken in two main steps, namely providing a philosophical analysis of privacy concepts and specifically applying the PGC.

To apply the PGC, the need to concentrate on the generic conditions of agency (GCA), which are 'simply whatever is/ might be necessary for action as such or successful action in general',[1] must be considered. The focus of this thesis is directly related to privacy, since the right to privacy is the main (yet not the only) fundamental right regarding data protection. To achieve the goal of the chapter, therefore, the starting point will be the philosophical analysis of privacy concepts in order to assist further progress. When these concepts are appropriately understood, they can enable us to see what is equitable and what is inequitable in the positions.

The second step will switch to the question of how to specifically apply the PGC to the central issue of this thesis, i.e., how to strike a balance between competing rights. According to T. Alexander Aleinikoff, '[t]he metaphor of balancing refers to

[1] Deryck Beyleveld and Roger Brownsword, *Consent in the Law* (Hart Publishing 2007) 50.

theories of constitutional interpretation that are based on the *identification, valuation, and comparison* of competing interests (emphasis added).'[2] Applying a theoretical framework as a balancing test, therefore, needs to deal with three tasks: to identify, evaluate and compare competing interests. Based on the PGC, in weighing competing rights and interests, the necessary steps are: (1) specifying what this right covers (identification stage); (2) asking which of these are the GCA and at what level (evaluation stage); and (3) deciding which rights can override the other rights (comparative stage).

In this respect, this section will firstly address the right to privacy granted by Article 8 of the ECHR as an example of specific application of the PGC and thus subsequently identify the protected rights. This is because, as we shall see, there is a need to interpret the Data Protection Directive in a manner which is compatible with the ECHR.[3] The ECHR, however, does not provide any explicit guidance to assess how to strike a balance between the rights granted. Besides, it does not grant the PGC official standing. The concern of this stage is thus to examine whether the ECHR is in line with the PGC.

Secondly, the need to evaluate the rights at issue in the light of the GCA can be satisfied by examining whether the violation of generic rights is permitted or justifiable under the exemptions listed in Article 8(2). Lastly, to decide which generic rights take precedence over other generic rights in case of conflict, the PGC offers the criterion of degrees of needfulness for action. This criterion will be examined to show whether it is capable of providing the added value that the proportionality principle

[2] T. Alexander Aleinikoff, 'Constitutional Law in the Age of Balancing' (1987) 96 Yale Law Journal 945.
[3] Paul Craig and Gráinne De Búrca, *EU Law: Text, Cases and Materials* (5th edn, OUP 2011) 366-367. For discussion in detail, see: section 5.2.1.3.1.

under the ECHR regime cannot. Then, we shall present a real-life case closely connected with the main issue of the thesis.

4.2 Philosophical Analysis of Privacy Concepts

4.2.1 Defining Privacy?

What is 'privacy'? It is of no surprise that discussions usually start with some common adjectives for the concepts of privacy: complex, vague, disarray, equivocal, etc. For example, in *the Right of Privacy*, Richard A. Posner starts his first sentence of the article with '[t]he concept of "privacy" is elusive and ill defined.'[4] Daniel Solove opens his contribution *Understanding Privacy*[5] by using 'Privacy: A Concept in Disarray' as the title of the opening chapter, in which he remarks that '[n]obody can articulate what it means'. [6] Commentators even argue that '[p]rivacy is a notoriously elastic and equivocal notion'[7] because it has a 'protean capacity to be all things to all lawyers.'[8]

In philosophical discussions,[9] some approaches to privacy are sceptical, mainly contending that privacy is merely analysable or reducible to the claims of others. Two

[4] Richard A. Posner, 'The Right of Privacy' (1978) 12 Georgia Law Review 393. The essay pays its attention on the law and economics of informational privacy, arguing that the trend of the privacy protection of the individual is 'the opposite of what one would expect if efficiency considerations were motivating privacy legislation.' Ibid 422.
[5] Daniel J. Solove, *Understanding Privacy* (Harvard University Press 2009). The ideas of this American privacy advocate will be presented and discussed in the later Chapters of this thesis.
[6] Ibid 1.
[7] Hilary Delany and Eoin Carolan, *The Right to Privacy: A Doctrinal and Comparative Analysis* (Thomson Round Hall 2008) 4.
[8] Tom Gerety, 'Redefining Privacy' (1977) 12 Harvard Civil Rights-Civil Liberties Law Review 234. For other similar comments, see: Daniel J. Solove and Paul M. Schwartz, *Informational Privacy Law* (3 edn, Aspen Publishers 2009) 41.
[9] For a rather detailed discussion, see: Graeme Laurie, *Genetic Privacy: A Challenge to Medico-Legal Norms* (CUP 2002) 6-8, 28-85. Also, Kenyon Mason and Graeme Laurie, *Mason and McCall Smith's Law and Medical Ethics* (8th edn, OUP 2011) 224-226.

main arguments of this account have been distinguished:[10] first, privacy can actually be expressed without referring to privacy at all; second, as Schoeman puts it: 'theorists who defend privacy fail to give sufficient weight to the socially and individually demoralizing aspects of a society in which respect for privacy is institutionalized.'[11]

Judith Jarvis Thomson is said to be amongst the most famous and influential scholars of the reductionist school.[12] She argues that most privacy claims actually can be well characterised in terms of other general liberty interests, in particular property rights or rights in respect of the person.[13] Additionally, some commentators have offered alternative versions of this argument. For example, while having much in common but being slightly weaker than Thomson's argument, Russell Brown suggests that due to the confusing use of privacy employed by the courts, the right to privacy should be better understood as the product of the legal concept of exclusivity.[14] Apart from these views, Posner uniquely presents his economic critique in which he argues that privacy is inadequately protected.[15]

It has been correctly argued that, however, the sceptical approach of privacy cannot work properly due to the lack of 'widespread culture, linguistic or conceptual understanding'[16] of privacy. Moreover, though a new right to privacy does not have a

[10] Ferdinand Schoeman, 'Privacy: Philosophical Dimensions' (1984) 21 American Philosophical Quarterly 209-210.
[11] Ibid.
[12] Delany and Carolan (n 7) 6. Also: Judith DeCew, 'Privacy' The Stanford Encyclopedia of Philosophy <http://plato.stanford.edu/archives/fall2008/entries/privacy/> accessed 21 Feburary 2011 *The Stanford Encyclopedia of Philosophy (Fall 2008 Edition)*, Edward N. Zalta (ed.) <http://plato.stanford.edu/entries/privacy/> assessed on 01 January, 2011.
[13] Judith J. Thomson, 'The Right to Privacy' (1975) 4 Philosophy and Public Affairs 295-314.
[14] Russell Brown, 'Rethinking Privacy' (2006) 43 Alberta Law Review 589. Russell Brown's approach is termed as the 'substitutive approach' by Delany and Carolan, see: Delany and Carolan (n 7) 5-6.
[15] Richard A. Posner, *The Economics of Justice* (Harvard University Press 1981).
[16] Delany and Carolan (n 7) 6. For example, in his article *The Right of Privacy*, Posner considers merely **parts** of informational privacy, as the study of information has become a crucial field of economics. Posner, 'The Right of Privacy' 393.

clear foundation in most *old* constitutions such as the US Bill of Rights, the French Declaration of Rights 1789, it is argued that there is a conceptually coherent concept of privacy.[17] The later amendments on constitutional documents and the international human rights instruments do support this new trend.[18] This argument is more persuasive in the modern technological era in which the debate around privacy concerns dramatically is rife in both academic and practical fields. In sum, without sufficient justification that privacy derives from other types of protected rights,[19] the reductionist theories suffer from the inability to capture developing dimensions of privacy.[20]

On the other hand, there are theorists defending the fundamental value of privacy interests.[21] It should be noted that any discussion of such an approach must deal with the question of how to specifically look at the concept of this claim. To be more specific, to define the concept of privacy is to extract an image of privacy describing what makes it clearly different from other ideas.[22] This should include common ideas held under the rubric of privacy. In this regard, Solove observes that 'traditional'[23] method of conceptualising privacy is to locate a category encompassing the essence of privacy which is separate from other conceptual categories.[24] With this in mind, six general types of conceptions of privacy are distinguished:[25]

---

[17] Judith DeCew, *In Pursuit of Privacy: Law, Ethics, and the Rise of Technology* (Cornell University Press 1997).
[18] Eric Barendt, 'Ptivacy as a Constitutional Right and Value' in Peter Birks (ed), *Privacy and Loyalty* (Claredon Press 1997) 8.
[19] Julie Inness, *Privacy, Intimacy, and Isolation* (OUP USA 1992) 36.
[20] For more detailed critics and responses to reductionists, see: Amy L. Peikoff, 'The Right to Privacy: Contemporary Reductionists and Their Critics' (2006) 13 Virginia Journal of Social Policy and the Law 474, cited from citation 127 in Solove, *Understanding Privacy* 38.
[21] This approach is termed the 'intuitionist approach,' see: Delany and Carolan (n 7) 6.
[22] Solove, *Understanding Privacy* 13-14.
[23] In Solove's contributions he suggests a 'new' method to conceptualise privacy. See: ibid. Also, Daniel J. Solove, 'Conceptualizing Privacy' (2002) 90 California Law Review 1087-1155.
[24] Solove, *Understanding Privacy* 14-15.
[25] Ibid 12-13. Also, Solove, 'Conceptualizing Privacy' 1087. Similar discussion on the conceptions of

1. The right to be let alone (the vary famous view addressed by Samuel Warren and Louis Brandeis which is often considered as the foundation of American privacy law);[26]
2. Limited access to the self (the ability to remove oneself from unwanted access by others);[27]
3. Secrecy (hiding from others);
4. Control over personal information (the ability to control over personal information);
5. Personhood (the protection of an individual's moral and physical integrity); and
6. Intimacy (to control one's intimate relationships).

Applying the method of conceptualising, each type of conception should be capable of maintaining its coherence by encompassing essential ideas and uses of privacy. For example, scholars who suggest that the concept of privacy is equivalent to a situation in which one intends to be let alone can encompass essential ideas such as limited access to the self (in order to be let alone), secrecy, control personal information (which is an essential instrument to satisfy the purpose of being let alone).

Each of these types, however, as Solove indicates, falls short of providing a full account of privacy. The influential inspiration of Warren and Brandies, for instance, 'fails to provide much guidance about what privacy entails.'[28] This is because the conception itself does not offer an approach for dealing with 'the matter how one should be let alone.'[29] As regards the inaccessibility point of view, which extends

privacy, see: Charles Fried, 'Privacy' (1968) 77 Yale Law Journal 483-493.
[26] Samuel Warren and Louis Brandeis, 'The Right to Privacy' (1890) 14 Harvard Law Review 193-220.
[27] This conception is also termed as 'inaccessibility.' See: Delany and Carolan (n 7) 8-9.
[28] Solove, *Understanding Privacy* 17.
[29] Ibid.

more broadly than being let alone, embracing freedom from interference from both public and private spheres, the problem is on its inapplicability to all situations. Thus, as Delany and Carolan argue, the inaccessibility concept of privacy suffers from an inability to explain 'far more complex and multi-faced questions of social existence'[30] encompassed by privacy.

So, what will the PGC say about privacy? Is privacy a type of the generic conditions of agency?

As indicated in Chapter 3, the needs of agency are generic only if 'they are prerequisites of an ability to act at all or *with any general* chances of success.'[31] Most theorists consider privacy as essential to act at all or at least improve the chance of success[32] – regardless of whether it is understood as having an intrinsic or instrumental value.[33] Even if some theorists who are in favour of the sceptical accounts of privacy and argue against both 'the coherence thesis and the distinctiveness thesis,'[34] the other relevant rights such as property rights still fall

[30] Delany and Carolan (n 7) 9.
[31] Deryck Beyleveld and Roger Brownsword, *Human Dignity in Bioethics and Biolaw* (OUP 2001) 70.
[32] For example, Charles Fried puts it: 'The conception of privacy as a necessary context for love, friendship and trust depends on a complex account of these concepts, and they in turn depend on the more general notions of morality, respect and personality.' Fried (n 25) 478. He goes on to address that '[t]he principle of morality does not purport to represent the highest value in a person's economy of values and interests. It necessarily assumes that persons have a variety of substantive values and interests and it is consistent with a large range of ethical systems which rank these values and interests in many different ways. It functions rather as a constraint upon systems and orderings of values and interests, demanding that whatever their content might be, they may be pursued only if and to the extent that they are consistent with an equal right of all persons to a similar liberty to pursue their interests, whatever they might be. Thus the principle of morality, far from representing a complete system of values, establishes only the equal liberty of each person to define and pursue his values free from undesired impingements by others. The principal of morality establishes not a complete value system but the basic entitlements of persons vis&-vis each other.' See: Charles Fried, 'Natural Law and the Concept of Justice' (1964) 74 Ethics 237-250.
[33] As a matter of fact, intrinsic and instrumental value of privacy need not be mutually exclusive. See: Solove, *Understanding Privacy* 84.
[34] Ferdinand Schoeman terms the question which asks: 'does an analysis of privacy in terms of a variety of interests rather randomly associated do justice to our conception of privacy' as the 'coherence issue.' He terms the question which asks: 'does an analysis of privacy in terms of other interests point to anything distinctive about privacy, in contrast to other values we find it important to protect?' as the 'distinctiveness issue.' Schoeman (n 10) 205.

under the scope of generic rights.

Alan Gewirth who set out the PGC dealt with privacy in his contribution. He argues that privacy falls within the concept of generic rights. In his article *The Basis and Content of Human Rights*, he addresses that:[35]

> Besides these three components of the right to well-being, the human rights also include the right to freedom. This consists in a person's controlling his actions and his participation in transactions by his own unforced choice or consent and with knowledge of relevant circumstances, so that his behaviour is neither compelled nor prevented by the actions of other persons. Hence a person's right to freedom is violated if he is subject to violence, coercion, deception, or any other procedures which attack or remove his informed control of his behaviour by his own unforced choice. This right includes having a sphere of personal autonomy and *privacy whereby one is let alone by others unless and until he unforcedly consents to undergo their action*. (emphasis added)

It seems that, however, the right to be 'let alone' is hardly the whole map of the concept of privacy, as it is merely a general type of conception of privacy. Nevertheless, this right can arguably be read in a broader sense. For example, limited access to the self, secrecy, control over one's personal information, and control over one's intimate relationships, may be interpreted as falling under the heading of 'the right to be let alone' as Gewirth defined.

However, such interpretation cannot cover concepts relating to some end or purpose constituting an agent's reason for acting, e.g., the agent's bodily integrity/ personhood (including her/ his/ its physical and moral integrity) and private

[35] Alan Gewirth, 'The Basis and Content of Human Rights' (1979) 13 Georgia Law Review 1159.

environmental spaces (shelters). This is because, as Gewirth divides the generic needs into two categories, namely voluntariness (or, generic freedom) and purposiveness (or, generic well-being),[36] privacy seems to be placed under the voluntariness category of generic needs, which is regarded as instrumental to purposiveness.[37]

Indeed, Beyleveld and Brownsword argue that there is no need to distinguish these two categories.[38] Two reasons are provided. Firstly, this enables the essence of the argument for the PGC to be presented simply in the light of the abstract category of generic needs. Secondly, this can 'leave specification of the generic needs (both abstract and concrete) to application of the PGC.'[39] This is particularly important in identifying the problem of privacy at issue.

Overall, in terms of the method of conceptualising, each conception of privacy is either too narrow and thus too restrictive, or too broad and thus too vague.[40] Even though Solove tried to propose a 'pragmatic privacy' theory to reconstruct privacy, which aims to 'shift the discussion from elucidating the inherent meaning of the term "privacy" to discussing the nature of certain problems'[41] by applying the 'taxonomy' understanding of privacy,[42] it has been argued that his model is 'logically circular' and fails to 'provide a coherent account of privacy.'[43] However, it does not follow that, as claimed above, one should therefore accept the reductionist theories which tend to

[36] Alan Gewirth, *Reason and Morality* (University of Chicago Press 1978) 27. The former one means that its performance is under an agent's aforementioned control; the latter means that the agent acts for some end or purpose that constitutes his reason for acting.
[37] Gewirth argues that '[a]lthough voluntariness or freedom, unlike purposiveness, is not conceptually tied to ends or purposes, the agent's control of his own behaviour serves, and is at least sometimes perceived by him as serving, as a means to attaining his ends.' Ibid 52.
[38] Beyleveld and Brownsword, *Human Dignity in Bioethics and Biolaw* 71, cite 4.
[39] Ibid 71.
[40] Solove, *Understanding Privacy* 37. For the other observations and comments of conceptions of privacy, see: ibid 21-37.
[41] Ibid 106.
[42] Ibid 39-77, 101-170.
[43] Delany and Carolan (n 7) 10.

consider the right to privacy as hardly distinguishable from a general right to liberty. Instead, to protect the individual against high-handed interference by others, it is rather unwise to tag or limit the concept of privacy.

4.2.2 The Value of Privacy

Analysing and conceptualising the understanding of privacy should involve both the entailments and the value of privacy. An assessment of the interests and values brought about by privacy is likely to assist in analysing concepts of privacy from a theoretical angle. This is because, as Delany and Carolan put, '[i]f we can understand the reasons why privacy is protected, we may be in a better position to devise a legal regime which is capable of achieving this end.'[44]

Why is privacy worth protecting? Again, it is unsurprising that since there are multiple conceptions of privacy, a variety of theses have been offered by theorists. A brief overview regarding the reasons for cherishing privacy provided by scholars and practitioners can be found in Solove's contribution:[45]

- Promotes human well-being;
- Is vital to self-development;
- Creates and improves intimate relationships; and
- Is essential for democracy.

The values in the above list are by no means an exhaustive taxonomy. On the

[44] Ibid 11.
[45] Solove, *Understanding Privacy* 79-80.

other hand, critiques to privacy can also be listed: [46]

- Threats society, community and solidarity;
- Impedes social control;
- Makes it difficult to establish trust and judge people's reputations;
- Shrouds the abuse and oppression of women at home (by feminist scholars);
- Is a past-time value; and
- Conflicts with the freedom of information and other values.

To understand why writers elaborate on the value of privacy in such a way, how their theories value privacy must be understood. Philosophers and ethicists defend the value of privacy through different motivations.[47] For example, the consequentialist or instrumentalist theories, by holding that 'the ends justify the means,' assume that a morally right act will produce positive consequences. This shares similar ideas to the Utilitarian theories when assessing the value of privacy. This claim, which has been applied in the US courts, tends to consider that personal privacy is hardly enough to outweigh a social good such as the value of freedom of expression.[48] Under the applications of Utilitarianism, scholars argue that individuals would be more willing to seek medical attention and participate in medical research if they could do so privately.[49]

Indeed, Utilitarian theories focus on collective privacy rather than on personal

[46] Ibid 80-83. Also, Schoeman (n 10) 199.
[47] Similar view on the English common law on confidence, see: Shaun D. Pattinson, *Medical Law and Ethics* (2nd edn, Sweet & Maxwell Limited 2009) 196-197.
[48] Delany and Carolan (n 7) 12.
[49] Anita Allen, 'Privacy and Medicine' The Stanford Encyclopedia of Philosophy <http://plato.stanford.edu/archives/sum2009/entries/privacy-medicine/> accessed 21 February 2011 *The Stanford Encyclopedia of Philosophy (Summer 2009 Edition)*, Edward N. Zalta (ed.) < http://plato.stanford.edu/entries/privacy-medicine/> assessed on 01 January, 2011.

privacy. To seek the best balance of utility over disutility, it values privacy in order to achieve the maximum good in general. As individual interests can be put together and meaningfully compared, corporate privacy and other 'greater' social values should therefore override personal privacy.

On the other hand, deontological (rights-based as well as duty-based) theories, holding that the promotion of privacy is beneficial to respecting the value of human dignity and autonomy, tend to agree that concepts of privacy should be treated as 'a value which is inherently deserving of protection.'[50] Examples[51] can be found in contributions by philosophers such as Stanley Benn,[52] Julie Inness,[53] and Beate Rössler.[54] It should be noted that the Kantian approach is regarded as central to deontological moral theories. Charles Fried, for instance, classifies his assessment of the value of privacy as Kantian because 'it requires recognition of persons as ends, and forbids the overriding of their most fundamental interests for the purpose of maximizing the happiness or welfare of all.'[55]

Furthermore, most of their work focuses on individual autonomy and autonomy as a social value. The 'autonomous individual' refers to the ability of an individual to control access to their self[56] by their free will.[57] 'Autonomy as a social value' mainly presents the other-regarding characteristic of an autonomous individual, which 'depends on a complex network of social mores and expectations.'[58] In her broadly

[50] Delany and Carolan (n 7) 12.
[51] Solove, *Understanding Privacy* 85.
[52] Stanley I. Benn, 'Freedom, and Respect for Persons' in J. Roland Pennock and J. W. Chapman (eds), *Nomos XIII: Privacy* (Atherton Press 1971) 2, 26.
[53] Inness (n 19) 95.
[54] Beate Rössler, *The value of privacy* (Polity Press 2005) 117.
[55] Fried, 'Privacy' 478.
[56] James Rachels, 'Why Privacy is Important' (1975) 4 Philosophy and Public Affairs 326.
[57] Delany and Carolan (n 7) 14.
[58] Ibid. For example, Charles Fried considers privacy as that 'aspect of social order by which persons control access to information about themselves. How this control is granted to individuals and the means for bringing about the social structures which express the notion of privacy have not been of

cited essay *Coercing Privacy*,[59] Anita Allen, sharing other nonconsequentialists' views on privacy, claims that privacy 'has value relative to normative conceptions of spiritual personality, political freedom, health and welfare, human dignity, and autonomy.'[60] She continues her argument by remarking that '[t]o speak of "coercing" privacy is to call attention to privacy as a foundation, a precondition of liberal egalitarian society. Privacy is not an optional good, like a second home or an investment account.'[61] In terms of her view on privacy, it seems that an agent cannot give away the exercise/ benefit of that right. Recalling the above theorists who consider privacy as an ability to control personal information, her view on the right to privacy may be considered as either signing up a duty-based or an interest-conception agenda.

4.3 How to Apply the PGC: Article 8 of the ECHR

4.3.1 Some Remarks on the Application of the PGC

Gewirth distinguishes two different types of application of the PGC: direct and indirect.[62] In the former type of application, the requirement of the PGC (that agents ought to act in accordance with the generic rights of all agents) is 'imposed upon the interpersonal actions of individual persons.'[63] In this regard, it involves application of the criterion of degrees of needfulness for action to resolve conflicting cases.

In light of the right to privacy, the direct application of the PGC is regarded as

direct concern.' Fried, 'Privacy' 493. See also, Rachels (n 56) 326-331.
[59] Anita Allen, 'Coercing Privacy' (1999) 40 William and Mary Law Review 723-757.
[60] Ibid 738.
[61] Ibid 740.
[62] Gewirth, *Reason and Morality* 200.
[63] Ibid 200.

deontological consequentialism. [64] The PGC is a consequentialism with regard to the procedure of judging actions according to their consequences for the generic rights of agents. [65] However, this character must not be confused with Utilitarian consequentialism, as the PGC concerns the generic rights. Specifically, a generic harm caused by an action against the other agent can be justified under the PGC not because its consequences will achieve the maximum good, but as the action will correct or prevent such a generic harm (in a precautionary sense), and only if it is clear that the harm cannot otherwise be removed.[66] In this light, it is possible for other fundamental rights and freedoms to override the right to privacy. However, it is noted that 'corporate privacy' or other collective interests should not be able to override personal privacy (as required by the utilitarian approach).

It is noted that there are limits to the direct application of the criterion of degrees of needfulness for action. for example, diffculties arise when comparing the rights of an apparent agent with an apparent non-agent (e.g., a new-born baby) when:

(1) the same generic interest held by the two sides is not in conflict; or
(2) the apparent agent's less important generic interest (lower degree of needfulness for action) and the apparent non-agent's higher degree of needfulness for action are in conflict.

[64] Ibid 216.
[65] Ibid, see also, Beyleveld and Brownsword, *Consent in the Law* 56.
[66] Gewirth, *Reason and Morality* 216.

This is because, as Beyleveld notes, this weighting requires a specific value 'to be assigned to the precautionary probability of the apparent non-agent being an agent for which there is no obvious dialectially necessary answer.'[67]

In this regard, there must be rules governing agents' interactions in a complex society to deal with difficulties described above. An indirect application of the PGC can assist. The PGC's requirements are indirectly imposed upon the interpersonal actions of agents through the 'mediation of various social rules that govern multiperson activities and institutions, and the requirements of these rules in turn are imposed upon the actions of individuals who participate in the activities and institutions in accordance with their governing rules.'[68] These social rules include international and domestic human rights instruments. Again, it should be noted that these international/domestic human rights instruments must conform to the PGC and be structured in line with the GCA.

A preconditioned question thus must be asked before identifying the rights covered by the jurisdiction at issue: is the ECHR in line with the PGC? Adopting Beyleveld and Brownsword's insight, I argue that the ECHR is fully (at least broadly) in line with the PGC. This is because, based on the dialectically contingent justification, the interpretation of international human rights instruments must conform to the PGC.[69] Moreover, since: (1) Stage I of the dialectically necessary argument concludes that 'my having the generic conditions for agency is categorically good for me'; (2) the preamble of the ECHR considers the Universal Declaration of Human Rights, which declares that '[a]ll human beings are born free and *equal in*

[67] Deryck Beyleveld, 'The Principle of Generic Consistency as the Supreme Principle of Human Rights' (2012) 13 Human Rights Review 16. Also, Beyleveld and Brownsword, *Human Dignity in Bioethics and Biolaw* 255-258.
[68] Gewirth, *Reason and Morality* 200.
[69] See: section 3.4.

dignity and rights' (emphasis added); and (3) Article 1 of the ECHR requires that the Member States secure to *everyone* within their jurisdiction the rights and freedoms defined in the context of the ECHR; it *seems* that the ECHR is in line with the PGC.

However, this argument is not yet convincing enough. This is because the reasons illustrated above can only show that any agent who considers that any human being has a human right to do anything must consider that all human beings have equal rights to the GCA. This is not to say that any agent who considers that any human being has a human right to do anything must accept the PGC. It must be noted that 'only that acceptance of human rights under the will conception of rights requires acceptance of the PGC.'[70] This is because the PGC operates on the basis of the will conception. This can also be understood by reading stage II of the dialectically necessary argument. Nevertheless, as I have presented in Stage II of the alternative argument and as we shall see in the following subsection, the interpretations given by the ECtHR are in line with the idea that generic rights are under the will-conception rather than the interest-conception.

As regards ostensible agents, however, the ECHR itself does not *directly* protect the rights of the members of some special groups.[71] Nevertheless, based on the precautionary principle previously discussed, it is reasonable for these special groups to fall under the protection of the ECHR. It follows that duties to them do not correspond to the generic rights, but are justified *relatively to* them.

[70] Beyleveld and Brownsword, *Human Dignity in Bioethics and Biolaw* 82.
[71] Ibid 81. The recent extension of human rights to these members of minority groups is controversial. With respect to the ECHR, the protections to human embryos, which can be considered as potential partial agent, for example, are indirectly guaranteed by Convention for the Protection of Human Rights and Dignity of the Human Being with regard to the Application of Biology and Medicine: Convention on Human Rights and Biomedicine (1997). See: < http://conventions.coe.int/Treaty/en/Treaties/Html/164.htm>. Assessed on 12 November, 2010.

4.3.2 The Rights Protected by Article 8(1) of the ECHR

The interests protected by Article 8(1) of the ECHR include: (1) private life; (2) family life; (3) home; and (4) correspondence. None of these interests, however, is self-explanatory in the simple wording of this Article. Nevertheless, the notion of Article 8(1) has been given an extended meaning consistent with 'social and technical developments' by the ECtHR interpretations.[72] The widening categories of Article 8(1) embrace issues including personal status and identity, moral or physical integrity and intellectual freedom, privacy in public and private space, personal and business communications, collection and use of personal information, sexual activities, sexual identity and gender, ethical identity, rights to one's image, social life, and the enjoyment of personal relationships.[73]

The following discussion of the breadth of the rights covered by Article 8 of the ECHR will be classified in three main categories: (1) spatial privacy; (2) decisional privacy; and (3) informational privacy.[74] This differentiation is based on the remark in which Anita Allen proposes in her influential article *Taking Liberties: Privacy, Private Choice, and Social Contract Theory*.[75] The reasons why I adopt her identification are:

---

[72] David Harris and others, *Harris, O'Boyle & Warbrick: Law of the European Convention on Human Rights* (2nd edn, OUP 2009) 361-362. *Peck v UK* (2003) 36 EHRR 41 para 57. Also, *Niemietz v Germany* (1992) 16 EHRR 97 para 29; *Pretty v UK* 2346/02 (App no 2346/02) 2002-III 35 EHRR 1 para 61; and *P.G. & J.H. v. U.K.* (App no 44787/98) ECHR 2001-IX para 56.

[73] See: David Feldman, *Civil Liberties and Human Rights in England and Wales* (2nd edn, OUP 2002) 527-536. Also, Harris and others (n 72) 364-371; Robin White and Clare Ovey, *Jacobs, White and Ovey, The European Convention on Human Rights* (5th edn, OUP 2010) 358-401. *S and Marper v UK* (App nos 30562/04 and 30566/04) ECHR 4 (App nos 30562/04 and 30566/04) ECHR 4 para 66.

[74] There are other ways of categorisation. For example, Mason and Laurie contend that privacy consists of two aspects only: informational privacy and spatial privacy. See: Mason and Laurie (n 9) 224-225.

[75] Anita Allen, 'Taking Liberties: Privacy, Private Choice, and Social Contract Theory.' (1987) 56 Cincinnate Law Review464-466. Also, Allen, 'Coercing Privacy' 723. In fact, this method of distinguishing dimensions of privacy is not a stranger in the international privacy literatures. See for example: Rössler. In Rössler's contribution, she suggests three dimensions of privacy, namely

1. There is an absence of a clear articulation in the ECtHR jurisprudence regarding categories on which the Strasbourg Court relies. Although there are indeed some contributions that try to identify the Court's observation about the concepts and scope of Article 8,[76] the Court itself has recognised no official categorisation;
2. However, in addressing issues regarding the plethora of different rights covered by Article 8, a clear categorisation simplifies the analysis ; moreover,
3. There is no limit in relation to the classification of concepts of privacy on the basis of the PGC; and
4. Allen's categorisation is followed by a majority of Formosan scholars, practitioners and the constitutional interpretations.[77]

In this regard, the adoption of her categorisation can be used as a general application ensuring the consistency of this thesis. Several points should be noted before going on: first, since the interpretation of Article 8(1) given by the Court is 'dynamic and continuous,'[78] which is not susceptible to exhaustive definition; the discussion below only involves *present* types of issues. Secondly, the variety rights covered by Article 8 are closely related to each other, some of which are 'connected with each other and some overlap.'[79] Thirdly, after indicating a rich diversity of rights that fall under the heading of the right to private life covered by Article 8, only selected issues focusing on the specific forms of privacy that are relevant to the thesis will be discussed further.

---

decisional privacy, information privacy and local privacy.
[76] E.g., N. A. Moreham, 'The Right to Respect for Private Life in the European Convention on Human Rights: a Re-examination' (2008) 1 EHRLR 44-79.
[77] Section 5.4.
[78] Feldman (n 72) 527.
[79] Harris and others (n 72) 361.

Spatial Privacy (I): Moral and Physical Integrity

This sub-category of the right to private life has been observed by the Strasbourg Court consistently. For example, a person's body integrity has been considered as 'the most intimate aspect of one's private life.'[80] In this connection the right to be free from physical and sexual assault and exposure, therefore, is said to be the first interest to fall within this sub-category.[81] In the *Y. F. v Turkey* Case the Court concludes that any interference with a person's physical integrity must be prescribed by law and requires the consent of that person. This attitude reiterates in cases such as *Pretty v UK*,[82] concerning assisted suicide, in which the Court notes that the concept of individual autonomy is of central importance. Similarly, in *Glass v UK*[83] the Court indicates that medical treatment in the face of parental oppositions interferes with the child's right to private life.

It must be noted that, although the requirement of harming against body integrity in Article 8 is not as strict as Article 3 of the ECHR, not every act affecting bodily integrity constitutes a violation of Article 8 rights.[84]

Spatial Privacy (II): Private Space

A number of cases regarding private space are frequently considered by the Strasbourg Court. These include the right not to be spied upon, watched, or harassed. The harm involved is usually caused by the controversy concerning surveillance or the interception of communications.[85] Situations normally take place with regard to

[80] E.g., *Y.F. v Turkey (App no 24209/94) ECHR 2003-IX*, para 33. Also, *X and Y v the Netherlands* judgment of 26 March 1985, Series A no 91, para 22.
[81] Moreham (n 76) 49.
[82] *Pretty v UK* paras 73-78.
[83] *Glass v UK* (App no 61827/00) 2004-II 39 EHRR 341.
[84] *Costello-Roberts v UK* (App no 13134/87) (1993) 19 EHRR 112 para 36.
[85] The right of not being spy on (surveillance and observation) might also be considered as within the

the collection and retention of personal data from governmental surveillance[86] with the view of securing national security and criminal defence.[87] Sometimes the harm can be also serious with respect to the private sector. A recent example is the UK phone-hacking scandal in July 2011, which involves the 'understandably attracted intense interest from politicians and the media whose daily business is power.'[88]

One crucial issue in relation to this category is how to understand the concept of 'a zone of privacy.' It is observed by Harris and others that this zone of privacy 'relates to the person whose private life is at issue' rather than the place where the interference occurs.[89] This closely involves and sometimes even overlaps with the definition of 'home' in Article 8. Similarly, although the Court defines the 'home' as 'usually be the place, the physically defined area, where private and family life develops and that the individual has a right to the quiet enjoyment of that area,'[90] the notion of it has been extended, for example, to include business premises where business is conducted from home.[91]

The interests protected by such a zone of privacy cover both the physical/ concrete enjoyments of residence there and those non-physical ones, such as noise, smells, or any forms of unpleasant emissions.[92] This sub-category of the right to private life thus also includes the right to have clean and quiet space to live in. The

---

category of physical and mental integrity. See: Moreham (n 76) 52-62.

[86] E.g., *Hewitt and Harman v UK* (App no 12175/86) (1992) 14 EHRR 657 concerning personal information stored by a secret police register, and *Amman v Switzerland* (App no 27798/95) (2000) 30 EHRR 843 concerning the surveillance of telephone calls of a Switzerland businessman by the public authorities.

[87] *Malone v UK* (App no 8691/79) (1985) series A no 82, 7 EHRR 14.

[88] Madeleine Bunting, 'Phone-hacking scandal is an outrage of human decency' *The Guardian* (14 July 2011) <http://www.guardian.co.uk/commentisfree/2011/jul/14/phone-hacking-scandal-ethics> accessed 14 July 2011.

[89] Harris and others (n 72) 368.

[90] *Giacomelli v Italy* 2006-XII, 45 EHRR 871 para 76.

[91] *Niemietz v Germany* para 30.

[92] *Hatton v UK* (2003) 37 EHRR 28 para 96. Also, *Lopex Ostra v Spain* (1994) Series A no 303-C, 20 EHRR 277, *Guerra v Italy* 1998-I, 26 EHRR 357, and *Giacomelli v Italy*.

Strasburg Court also found that Member States have positive obligations to adequately regulate private industries from polluting the environment in the *Hatton* Case.[93] In some cases, the right to private space/ home has been interfered with, for instance, violations of the right to respect one's home and correspondence,[94] as well as the right to be let alone.[95]

Decisional Privacy: Personal Status, Identity, and Autonomy

It is observed that 'the capacity of the individual to *determine* his identity' (emphasis added) is covered by the right to private life.[96] In this regard, this sub-category of rights covers a right both to develop personality and 'the relationships with other human beings and the outside world.'[97] This includes the establishment, development and enjoyment of one's social life and relationships with others, embracing multiple aspects of a person's physical and social identity,[98] such as[99]

1. Gender identification;
2. Sexual orientation and sexual life; and
3. Name and other means of personal identification and of linking to a family.

Transsexuals' official recognition [100] and family relationships [101] have been

[93] *Hatton v UK* para 98. It should be noted at the same time, however, the ECtHR does not always try to clearly articulate whether Member States have obligations in environmental cases due to the need of a wide margin of appreciation. See: Moreham (n 76) 66.
[94] *Klass and Others v Germany* (App no 5029/71) (1978) series A no 28, 2 EHRR 214 PC and *Malone v UK*.
[95] Harris and others (n 72) 378.
[96] Ibid 366.
[97] *S and Marper v UK* para 66. See also, *Burghartz v. Switzerland* 22 February 1994, Series A no 280-B, opinion of the Commission, para 47 and *Friedl v Austria* judgment of 31 January 1995, Series A no 305-B, opinion of the Commission, para 45.
[98] *Mikulić v. Croatia* (App no 53176/99) ECHR 2002-I para 53.
[99] *Bensaid v. the United Kingdom* (App no 44599/98) ECHR 2001-I para 47; *Peck v UK* para 57, *Burghartz v. Switzerland* para 24 (*mutatis mutandis*); and *Ü nal Tekeli v. Turkey* (App no 29865/96) ECHR 2004-X para 42.
[100] *B v France* (1992) 16 EHRR 1 para 62.
[101] For example, the relationship between parents and kids, see: *Rasmussen v Denmark* (1984) 7 EHRR 371 para 33; see: *Jäggi v Switzerland* (App no 58757/00) ECHR 2006-X 13 July 2006 concerning

adopted as falling within the scope of the right to private life in some Strasbourg cases. This right may be able to override other privacy interests. For example, the *Jäggi* case indicates that in order to exercise the interest of personal identity, proper access to relevant personal biometric data (such as a DNA test) is thus needed. Moreover, in *Odièvre v France*, the Court held that a system allowing *complete* anonymity for the mother throughout the birth and adoption process is able to strike a balance between the applicant's right to access information about his/her parent and competing interests.[102]

Secondly, the right to develop relationships with others undoubtedly involves the free choice to engage in sexual activities. In this regard, the Court considers that sexual relations represent the most intimate part of private life in the *Dudgeon* case.[103] Finally, the right to develop relationships with others also involves the right to respect one's 'family life' in Article 8. The Court appreciates the development throughout time of the notion of the 'family life.' It is now understood as extending beyond the idea of 'formal relationship and the family based on marriage' by the Court.[104] This includes the considerations with regard to, for example, children born outside the marriage (including the previous marriages or relationships), non-biological links between children and parents, same-sex partnerships, divorces, and relationships with extended family members such as siblings, grandparents-children and uncle-nephew.[105]

Informational Privacy: Collection, Retention and Access of Personal Information

---

individual's interest in discovering his parentage.
[102] *Odièvre v France* (2003) 38 EHRR 43 para 48.
[103] *Dudgeon v UK* (App no 7525/76) (1981) 4 EHRR 149, 165 para 52.
[104] Harris and others (n 72) 371-372. *Johnson v Ireland* Series A no 112 (1986) 9 EHRR 203 and *Marckx v Belgium* Series A no 31 (1979) 2 EHRR 330.
[105] Harris and others (n 72) 371-376.

Personal information, e.g., information with respect to a person's health and ethics identity,[106] and image of the individuals[107] is related to the elements of private life under the ECHR. It is established by the Court that collecting personal data (e.g., fingerprints and images) by public authorities/ policing powers without the data subject's valid consent (for instance, for facial images) will interfere with one's right to private life protected by Article 8(1).[108] Similarly, the establishment of national DNA databases, which collect and retain personal biometric data, has been declared by the ECtHR to be in violation of Article 8 in *S and Marper* case due to the blanket and indiscriminate power of police investigation.[109]

In general, Member States will need to provide further information in order to offer an 'effective and accessible' procedure for accessing 'all relevant and appropriate information'.[110] Specifically, for example, the Court concluded that Member States have a positive obligation under Article 8(1) with regards to proper access to personal data for issues such as threats to public health.[111]

Specific Forms of Privacy that Are Relevant to This Thesis

The main object of this thesis focuses on the emerging biometric and RFID technologies. Accordingly, after presenting a rich diversity of rights covered by the heading of the right to private life, I shall then focus on the specific forms of privacy that are relevant to the research question of this thesis.

---

[106] *Z. v Finland* (1998) 25 EHRR 371 paras 71 and 41.
[107] *Sciacca v. Italy* (App no 50774/99) (2005) ECHR 2005-I para 29.
[108] *Murray v UK* (App no 14130/88) (1994) 19 EHRR 191 concerning photographs collected by the police and *McVeigh, O'Neill and Evans v United Kingdom* (1981) 25 DR 15 concerning finger printings and photographs collected and stored by the police.
[109] *S and Marper v UK* para 125, also, *Goggins and Others v The United Kingdom* (App nos 30089/04, 14449/06, 24968/07, 13870/08, 36363/08, 23499/09, 43852/09 and 64027/09) 72.
[110] *McGinley and Egan v United Kingdom* (1998) 27 EHRR 1 para 101. Also, *Roche v United Kingdom* (2006) 42 EHRR 30 para 162.
[111] *Guerra v Italy*.

Obviously, the rights falling under the scope of informational privacy granting protection with respect to the collection, retention and processing of personal information are some of the particular forms of privacy at issue. In Chapter 2 we have seen that biometric data include various types of sensitive personal data, e.g., image data,[112] fingerprint data,[113] cellular data, and DNA data.[114] Moreover, these data may contain information with respect to health data[115] and ethical data. Such biometric samples and profiles are crucial elements relevant to private life. Hence, to collect, store, and process such data, including the sample and the profiles of them, is 'sufficiently intrusive to constitute an interference with the right to respect for private life set out in Article 8 of the ECHR.[116]

Moreover, the potential future use of the personal biometric information contained in the profiles, as the ECtHR notes, is 'relevant to a determination of the issue of whether there has been an interference.'[117] As regards the biometric samples, the subsequent use of the body parts in relation to the technologies at hand is included within the concept of the right to body integrity.[118]

To more specifically focus on the relevant forms of privacy rights and the justifications to their interferences, I will provide an example and further analysis in the following subsection.

The Right to Privacy Is as Positive as It Is Negative

On the basis of the outline and justifications to the PGC in the last chapter, we have

[112] *Sciacca v. Italy*.
[113] *Van der Velden v the Netherlands* (App no 29514/05), 7 December 2006 and *S and Marper v UK*.
[114] *Van der Velden v the Netherlands*, *S and Marper v UK*, and *W. v the Netherlands* (App no 20689/08), 20 January 2009.
[115] *Z. v Finland*.
[116] *Van der Velden v the Netherlands*.
[117] *S and Marper v UK* para 71.
[118] Section 6.3.1.

seen that generic rights entail both mutually negative and positive duties. Human rights upheld by the PGC can be protected in a negative way, in which the possession of negative rights entails negative duties of agents not interfering with one another's actions. On the other hand, positive generic rights entail mutual duties to provide assistance for agents who cannot attain generic needs by their own unaided efforts if they so wish.

What should be noted is that the imposed negative and positive duties are not removed by the complexities in 'large-scale modern societies.'[119] Moreover, the correlative negative and positive duties 'bear not only on individuals as recipients but also on the economic and political structures of whole societies.'[120] Consequently, the duties apply to situations not only with respect to individuals, but also where generic harm arises from social or institutional contexts of the States. However, it must be emphasised that it is crucial to distinguish between (a): negative and positive obligations of States; and (b): negative and positive rights of individuals (agents). It is noted that positive obligations of the state are obligations of the state to ensure that individuals enjoy these rights if they so wish. More specifically, positive obligations of the state, in effect, require public authorities to take the necessary but reasonable measures to safeguard given rights.[121] Such measures can be in law as well as in practice.[122] This is because the agents are the ultimate respondents of the rights holders of the generic condition of agency.[123] Yet these might only be negative rights, e.g., rights not to have their privacy not interfered with, rather than rights to be

[119] Alan Gewirth, *The Community of Rights* (The University of Chicago Press 1996) 34.
[120] Ibid 36, 41-42.
[121] *Hokkanen v Finland* Series A no 299-A (1994) 19 EHRR 139, and *Lopex Ostra v Spain.*
[122] *Vgt Verein Gegen Tierfabriken v. Switzerland* Application no 24699/94, Judgement of 28 June 2001 para. 45. Also, Jean-François Akandji-Kombe, *Positive obligations under the European Convention on Human Rights: A guide to the implementation of the European Convention on Human Rights* (Council of Europe 2007) 7.
[123] Gewirth, *The Community of Rights* 56.

assisted by other individuals to secure their privacy. Accordingly, positive obligations of the state are not the same thing as positive rights of individuals vis-à-vis individuals.

Arguably, moreover, the wording of the Convention itself provides that the rights under Article 8(1) may be subject to restrictions of Article 8(2), whereby states bear merely a negative obligation.[124] However, this is not always consistently upheld by the later Strasbourg jurisprudence. In *X and Y v the Netherlands*,[125] for example, the Court declares that 'in addition to this primary negative undertaking, there may be positive obligations inherent in an effective respect for private and family life…' This attitude is then consistently followed.[126] Accordingly, Member States have both negative and positive obligations by virtue of the ECtHR judgements.[127]

The positive obligation upon the member states rests on the duty to 'respect' Article 8(1). Member States must thus ensure the rights enshrined in Article 8(1) are protected *effectively* by adopting positive and well-designed measures.[128] Moreover, the Court also holds that the positive obligations under Article 8(1) can extend to private activities[129] and 'the realm of newer generational rights.'[130] In this regard, States are still recognised by the Court to enjoy a margin of appreciation to an extent that 'the notion's requirements will vary considerably from case to case.'[131] Therefore,

[124] *Lingens v Austria* Series A no 103 (1986) 8 EHRR 407 PC. Harris and others (n 72) 382.
[125] *X and Y v the Netherlands* para 23.
[126] E.g., *Airey v Ireland* Series A no 32 (1979) 2 EHRR 305 para 32 and *Von Hannover v. Germany* (App no 59320/00) (2004) ECHR 294. Also, Ian Leigh and Roger Masterman, *Making Rights Real: The Human Rights Act in its First Decade* (Hart Publishing 2008) 236-237.
[127] Feldman (n 73) 524-527. Also, Harris and others (n 72) 361-363. See, e.g., *Rees v UK* Series A no 106 (1986) 9 EHRR 56 para 37, *Gaskin v UK* Series A no 160 (1989) 12 EHRR 36 para 49.
[128] *Mosley v the United Kingdom* (App no 48009/08) judgement of 10 May 2011 para 106.
[129] *X and Y v the Netherlands* para 27. See: Alastair Mowbray, *The Development of Positive Obligations under the European Convention on Human Rights by the European Court of Human Rights* (Hart Publishing 2004). Also, Leigh and Masterman (n 126) 236, 248-252.
[130] Mowbray (n 129) 187.
[131] *Sheffield and Horsham v. the United Kingdom* (App nos 22985/93; 23390/94) Judgement of 30 July 1998 para. 52, and *Hokkanen v Finland* para 55. Also, Akandji-Kombe (n 122) 36.

the Strasburg Court rarely goes so far as to clearly indicate which appropriate positive measures a member party should take.[132]

The Will-conception of Rights

To avoid denying the recognition of human rights, it has been argued that any convention recognising human rights has to be interpreted in line with the PGC on the sufficient condition that the convention accepts human rights under the will-conception.[133] On the basis of the alternative argument addressed,[134] moreover, in combination of the acceptance of stage I endorse the dialectically necessary and the impartiality assumption, which is supported by the ECHR, that an agent ought to act in any other agent's GCA. This entails that an agent categorically ought to act with regards to any other agent's GCA in accordance with her/his/its will. Since the rights in respect to the GCA are accepted as compatible with the conclusion of stage I of the dialectically necessary argument, those rights implied by the ECHR (as well as other human rights instruments, e.g., the UDHR and the ICCPR) must be assigned under the will conception. Accordingly, agents (i.e. human agents with reference to the ECHR) possess their generic rights and can freely waive the *benefits* of such rights, unless they renounce claims for insisting on or using of benefits of rights results in endangering at least same ranking of generic rights of others.

In effect, the interpretations given by the ECtHR are indeed in line with the will-conception reasoning. For example, it is repeatedly recognised by the Strasbourg judgements that by collecting and processing any sensitive personal data, the data subject's explicit consent must be present (or justified by the exemptions).[135]

[132] Akandji-Kombe (n 121) 36.
[133] Beyleveld and Brownsword, *Human Dignity in Bioethics and Biolaw* 82.
[134] Secion 3.4.2.
[135] E.g., *Z. v Finland* and *MS v Sweden* (1999) 28 EHRR 313. See also, Deryck Beyleveld and Shaun D.

Furthermore, when dealing with reconciling competing rights to private life in conflicting circumstances, the Court considers that the individuals could waive confidentiality if they wish to.[136]

However, it is arguable that the Strasbourg jurisprudence has, on occasion, found against the will-conception. In *Laskey, Jaggard and Brown v UK*,[137] the applicants had been engaged in consensual homosexual activities involving violent sadomasochistic actions and were convicted for assault resulting in actual bodily harm. The ECtHR held that the actions of giving and receiving pain for sexual pleasure remained a violation of human rights even if consensual. Moreover, according to Lord Templeman in *R v Brown and Others*,[138] Article 8 of the ECHR was not breached by a law prohibiting violence which causes physical and psychological harm. It thus seems that the ECHR aims to protect certain essential interests of agents/humans, e.g., personal security. In this regard, agents cannot waive the interests protected by the rights. Nevertheless, it has been argued that this judgement ignores the reality with regard to the law of consent, 'both with respect to sexual relations and also in those relations of violence which are capable of being consensual.'[139] Moreover, this decision to 'accept the criminal nature of the acts before the court precluded any consideration of the nature of consent' has also been doubted.[140] In this respect, the Court does not conclusively rule against the will-conception.[141]

Thus, the exceptions occasionally set out by the Court, based on the coherence of

---

Pattinson, 'Moral Interests, Privacy, and Medical Research' in Michael Boylan (ed), *International Public Health Policy and Ethics* (Springer Netherlands 2008) 50-51.

[136] *Odièvre v France* para 49.

[137] *Laskey, Jaggard and Brown v UK* (1997) 24 EHRR 39.

[138] *R v Brown and Others* [1994] 1 AC 212, 237.

[139] Lesile Moran, '*Laskey v The United Kingdom*: Learning The Limits of Privacy' (1998) 61 Mod L Rev 83.

[140] Ibid.

[141] In fact, this decision is argued to be a judgement which makes 'disturbing reading.' Ibid 84.

applying the right-based approach, cannot be regarded as cases of application of the interest-conception. Rather, these special cases should be treated as based on the criterion of degrees of needfulness for action, where rights of other agents under the will-conception require the waiver of the rights in question to be overridden.

A Broad Concept of Article 8(1)

The very essence of the ECHR is the respect for fundamental rights and freedoms. However, how the Court judges whether a specific action falls within the scope of the guaranteed rights or freedoms 'might be open to question.'[142] The nature of fundamental rights and freedoms thus results in inconsistent interpretations regarding the scope of the enshrined rights: the right to privacy is included therein.

One should not forget the core purpose of an article when looking at the scope of the rights covered by any specific article under the EHCR. Take Article 8 as an example, the ECtHR identifies that 'the essential object of Article 8 is to protect the individual against arbitrary interference by the public authorities' in the *Hokkanen* case.[143] It is also underlined by the Court that the intention of Article 8(1) is to ensure that 'the development, *without outside interference*, of the personality of each individual in his relations with other human beings.' (emphasis added)[144]

With this in mind, it is unwise to ignore the extension of a right entailing the notion of respect. In other words, this narrow concept of privacy, which tries to link the rights covered by Article 8 of the ECHR to merely 'the right to privacy' with a sense of narrow interpreting, may produce inappropriate results. It is therefore

[142] Jeremy McBride, 'Proportionality and the European Convention on Human Rights' in Evelyn Ellis (ed), *The Principle of Proportionality in the Laws of Europe* (Hart Publishing 1999) 23.
[143] *Hokkanen v Finland* para 55.
[144] *Von Hannover v. Germany* para 50. See also: *Hokkanen v Finland* and *Botta v Italy* (1998) 26 EHRR 241 para 32.

unsurprising that the Court rejects this narrow interpretation. For example, the *Niemietz* Case points out that the Court tends to interpret Article 8 broadly under its jurisprudence:[145]

> '[r]espect for private life must also comprise to a certain degree the right to establish and develop relationships with other human beings,'…
>
> 'it would be too *restrictive* to limit the notion to an "inner circle" in which the individual may live his own personal life as he chooses and to exclude therefore entirely the outside world not encompassed within that circle.'[146]

One question, however, remains unresolved: does the Strasbourg Court possess absolute power in assessing the applicability of Article 8(1) of the ECHR? Although there is indeed a tension between the power of sovereignty owned by nation states and individual fundamental rights and freedom protected by the ECHR, Member States are not able to claim restrictions freely *without any limitation* on those protected rights after having signed and ratified the Convention.[147] Therefore, it is at least appropriate 'for the Court to impose procedural requirements on states' which violate interests protected by Article 8(1).[148]

Overall, the opinion of the ECtHR with respect to identifying whether a right is covered by Article 8, which considers that the right to private life is 'incapable of exhaustive definition,'[149] is in line with the broad conception of privacy. However, the Court does provide some guidelines to understand the definition and scope of the

[145] See: Deryck Beyleveld, 'Conceptualising Privacy in Relation to Medical Research Values' in Sheila AM McLean (ed), *First Do No Harm: Law, Ethics and Healthcare* (Ashgate Publishing 2006) 154-155. Also, Harris and others (n 72) 364-366.
[146] *Niemietz v Germany* para 29. Also, *Costello-Roberts v UK* para 6 and *Peck v UK* para 57.
[147] Feldman (n 73) 541.
[148] Ibid 542.
[149] Harris and others (n 72) 364.

primary aim of Article 8(1). Nonetheless, this approach is not clear enough. Two reasons can be given: first, the Court does not depend on an applicable theoretical framework and clear guidelines to deal with non-exhaustive and ill-defined definition of Article 8(1). Secondly, it is observed by David Feldman that:

> [t]he field is becoming considerably more complex because of developments information technology and the explosion in the range of legal rules which seek to regulate the use of information.[150]

This presents a problem for the Strasbourg Court and domestic courts: **is there a rationale to assist the ECtHR to identify those aforementioned rights?** This question shall be answered (together with another question set out in the next subsection) below.

4.3.3 The ECtHR Approach of Balancing Test

After identifying that the rights at hand fall under the scope of Article 8, the following steps are to evaluate and compare the rights at issue. Before doing so, however, one must examine how the ECtHR approach operates.

Article 8(2) and the Principle of Proportionality

The standard interpretative approach applied by the ECtHR to examine Articles 8-11 of the ECHR has been termed the 'constitutional approach' [151] or the

[150] Feldman (n 73) 531.
[151] Foundation for Information Policy Research, *Paper No. 4: The Legal Framework: an Analysis of the "Constitutional" European Approach to Issues of Data Protection and Law Enforcement* (UK Information Commissioner Study Project: Privacy & Law Enforcement, 2004) 9.

'interference-violation approach.'[152] Under this systematic approach, in terms of Article 8, the first step is to investigate whether an action amounts to interference with the rights protected by this article. This is then followed by assessing whether the violation is permitted or justifiable under the scope of the restriction or limitation laid down in Article 8(2), if any interference is found at the first stage. In other words, Article 8(2) offers limitations permitting the rights enshrined in Article 8(1) to be overridden by specified public interests as well as the fundamental rights and freedoms of other individuals. Hence, it is essential to explore the exempting conditions regulated in Article 8(2) in order to evaluate the level of protection afforded to such rights.

The exempting condition offered by Article 8(2) is *broadly framed*:

> There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

To understand this paragraph, the standard formula consistently followed by the Court can be presented in the sub-stages set out below:

(1) To assess whether any interference is 'in accordance with the law' or 'authorised by the law,'[153] two sub-principles can be distinguished. First, the interference must be 'governed by law,'[154] rather than any ordinary

[152] Stephen Kabera Karanja, *Transparency and Proportionality in the Schengen Information System and Border Control Co-operation* (Martinus Nijhoff Publishers 2008) 89.
[153] This review stage is also termed as the 'rule-of-law criteria'. See: Feldman (n 73) 536-537.
[154] Ibid 537.

administrative orders. Secondly, the law must be foreseeable by a rational agent.

(2) To assess whether any interference serves the purpose of the legitimate interests listed in the concerned article.

(3) To access whether any interference is 'necessary in a democratic society.'

The interference here can be either within or outside the scope of Article 8 since there are a number of rights covered in it. If any violation in question cannot be justified in the earlier sub-stage, then there is a violation incompatible with Article 8. If so, there is no need to move on to examine the further stages. With reference to the above formula, it seems to be possible to evaluate competing rights and interests: if any interference is justified, the right being violated is overridden in specific competing case at issue.

The last stage of the ECtHR balancing test approach requires the evaluation of the *principle of proportionality*.[155]

This principle, although not stated expressly in the ECHR itself, plays a central role in the case law of the Strasbourg Court[156] in order to strike a 'fair balance between the demands of the general interests of the community and requirements of the protection of the individual's fundamental rights.' [157] Additionally, the proportionality test is also applied, in some cases, as a method to determine whether a positive obligation has been met.[158] By using this criterion, the lower level of

[155] The principle of proportionality embraces three sub-principles, i.e., (1) suitability; (2) necessity; and (3) proportionality in the narrow sense. See: Lord Hoffmann, 'The Influence of the European Principle of Proportionality upon UK Law' in Evelyn Ellis (ed), *The Principle of Proportionality in the Laws of Europe* (Hart Publishing 1999) 107.
[156] E.g., *Handyside v UK* (1976) 1 EHRR 737 para 49.
[157] *Soering v UK* Series A161 (App no 14038/88) (1989) 11 EHRR 439 para 89.
[158] E.g., *Rees v UK* para 37, *Gaskin v UK* A 160 (1989) 12 EHRR 36 para 49. Also, Harris and others (n 72) 10-11.

competing right can be regarded as being overridden by the higher one. In the following case we shall see how this principle operates in practice.

The ECtHR Balancing Test Approach: the Marper Case

The proportionality test is applied at the ECtHR and most domestic courts in considering whether different treatment regarding limitation against a Convention right is objectively justifiable. The British courts, after the HRA, also accepted and employed the same approach to some extent.[159]

In the UK case of *R v Chief Constable of South Yorkshire*[160] the applicants argue under Articles 8 and 14 of the ECHR that 'the authorities had continued to retain their fingerprints and cellular samples and DNA profiles after the criminal proceedings against them had ended with an acquittal or had been discontinued.'[161]

In the House of Lords decision, Lord Steyn suggests a narrow concept of the right to private life holding that the mere retention of fingerprints and DNA samples did not interfere with Article 8. This is because, as his Lordship explains, there is *no* decision of the ECtHR on the question whether retaining fingerprints or samples might interfere with Article 8[162] and in any event, 'the trial process ought to weed out' the abuse of processing such data.[163]

As regards the proportionality test, his Lordship distinguishes five factors to

[159] E.g., *Ghaidan v Godin-Mendoza* [2004] 2 AC 557, 605; *R v Secretary of State for Work and Pensions* [2006] 1 AC 173, 193. For details on the recognition of the principle of proportionality and its relationship with the *Wednesbury* review, see: Paul Craig, 'Unreasonableness and Proportionality in UK Law' in Evelyn Ellis (ed), *The Principle of Proportionality in the Laws of Europe* (Hart Publishing 1999) 85-106. David Feldman, 'Proportionality and the Human Rights Act 1998' in Evelyn Ellis (ed), *The Principle of Proportionality in the Laws of Europe* (Hart Publishing 1999) 117-144.
[160] *R v Chief Constable of South Yorkshire* [2002] EWHC 478 (Admin), [2003] EWCA Civ 1275, and [2004] UKHL 39.
[161] *S and Marper v UK* paras 3, 12.
[162] *R v Chief Constable of South Yorkshire* [2004] UKHL 39 para 26.
[163] Ibid para 28.

support his view that the interference was proportionate to the purpose of preventing crime and protecting the right of others to be free from suffering the effects crime.[164] Lord Brown, meanwhile, suggests that '[t]he more complete the database, the better the chance of detecting criminals, both those guilty of crimes past and those whose crimes are yet to be committed,' and '[t]he larger the database, the less call there will be to round up the usual suspects.'[165]

With respect to the risks of future misuse (i.e., 'function creep' meaning that further unintended or unnecessary processing of personal data in a way incompatible with the original purpose for which it was collected), Lord Steyn holds the opinion that '[i]f future scientific developments require it (i.e., contemporary use of retained samples in connection with the detection and prosecution of crime), judicial decisions can be made, when the need arises, to ensure compatibility with the ECHR.'[166]

The House of Lords therefore concludes that there is an objective justification under Article 8(2). However, the ECtHR disagreed. First, with reference to Article 8(1), the Court holds a broad concept of privacy and concludes that the retention of fingerprints and DNA samples fall within the scope of right to private life.[167] Secondly, as regards to the proportionality test, the Court acknowledged that

> [t]he core principles of data protection require the retention of data to be proportionate in relation to the purpose of collection and insist on limited periods of

[164] Ibid paras 38-40. These 'factors' are: '(i) the fingerprints and samples are kept only for the limited purpose of the detection, investigation, and prosecution of crime; (ii) the fingerprints and samples are not of any use without a comparator fingerprint or sample from the crime scene; (iii) the fingerprints and samples will not be made public; (iv) a person is not identifiable to the untutored eye simply from the profile on the database, any interference represented by the retention being minimal; (v) and, on the other hand, the resultant expansion of the database by the retention confers enormous advantages in the fight against serious crime.'
[165] Ibid para 88.
[166] Ibid para 28. Lord Brown also agrees this viewpoint, see: ibid para 86.
[167] *S and Marper v UK* paras 77, 85-86.

storage.

> …the protection afforded by Article 8 of the Convention would be unacceptably weakened if the use of modern scientific techniques in the criminal-justice system were allowed at any cost and without carefully balancing the potential benefits of the extensive use of such techniques against important private-life interests.
>
> …any State claiming a pioneer role in the development of new technologies bears special responsibility for striking the right balance in this regard.[168]

The Court also identified that the margin of appreciation is narrowly applied in this case. Accordingly, the Court concluded that the retention of biometric data (fingerprints and DNA samples in this case) of suspected but not convicted individuals, owing to the 'blanket and indiscriminate nature of power' cannot satisfy the proportionality test, thus failing to strike a fair balance between the competing public and private rights and interests.[169]

The Problem of the ECtHR Approach

Here, on the basis of the same factors, the proportionality test can result in different consequences. Indeed, even in the same court, by applying the principle of proportionality there can be inconsistency in cases.[170] Therefore, it is unsurprising that a commentator contends that '[t]he weakness of this process is that it is capable of leading to different conclusions on the same facts as was demonstrated by the

[168] Ibid paras 107, 112.
[169] Ibid para 125.
[170] See *Odièvre v France* where the 'majority gave little heed to such considerations.' Harris and others (n 72) 11 citation 93. Cf. *R (on the application of GC) v The Commissioner of Police of the Metropolis* [2011] UKSC 21.

divergent views of the majority and the minority.'[171]

It can be argued that this is partly because of the supranational character of the ECtHR [172] and the demand of balancing the legal differences that reflect the complexities of political, economic and social factors. The rejection of a one-size-fits-all model, together with an 'increasing burden of proof' for individual applicants,[173] which may vary on the basis of the nature of the issues considered and related interests of individuals,[174] led to the tendency of the Strasbourg Court to opt for a wider margin of appreciation instead of a strict interpretation test when the facts of the case are more likely to be subject to local variations.[175]

When the Strasbourg Court adopts a margin of appreciation in deciding cases, which appears to be narrower if fundamental rights and freedoms of individuals are called into play, it leaves national courts to identify situations in relation to local conditions according to domestic legislations.[176] Nevertheless, it must be emphasised that the margin of appreciation doctrine does not give domestic courts an unlimited power of interpretation. [177] Instead, by applying this doctrine, the courts of the contracting states are subject to the European supervision. The limitation and scope of the guaranteed rights regulated in Article 8(2) has been further clarified in Article

[171] Mowbray (n 129) 130.
[172] McBride (n 142) 23.
[173] Ibid 29-30. For a more detailed description, see: George Letsas, *A Theory of Interpretation of the European Convention on Human Rights* (OUP 2007) 79-98.
[174] McBride (n 142) 28-34.
[175] Feldman, *Civil Liberties and Human Rights in England and Wales* 540.
[176] Ibid. Also, Harris and others (n 72) 12-13.
[177] *Handyside v UK*. Even though shared by majority of domestic population, some local moral convictions are still subject to European supervision, particularly within the area of most intimate aspects of private life. See e.g., *Dudgeon v UK* para 60, and *Norris v Ireland* (1989) 13 EHRR 186 para 45. Also, Lech Garlicki, 'The European Court of Human Rights and the "Margin of Appreciation" Doctrine: How much Discretion is Left to a State in Human Rights Matters?' in Cheng-Yi Huang (ed), *Administrative Regulation and Judicial Remedies 2010* (Institutum Iurisprudentiae, Academia Sinica 2011) 89-91.

52(1)[178] of the Charter of Fundamental Rights of the European Union.

Although the margin of appreciation is applied, the uncertainty of the proportionality applications still presents a problem for domestic courts trying to follow the Strasbourg jurisprudence: it is difficult for them to ascertain exactly how the ECtHR interprets the ECHR. This generates a series of problems for the European citizens: the inefficient legal procedure, the financial cost in order to wait for the 'final' decision and the uncertainty of developing rights and interests…etc.

Overall, the Strasburg approach of balancing test is unclear and inconsistent. This is because of the combination of: (1) the need of a wider margin of appreciation; (2) the limitation set out in Article 8(2) is broadly framed; and (3) the principle of proportionality lacks clear guidelines. Accordingly, this character does cause a significant problem: **it is difficult to ascertain exactly what local courts should be 'taking into account' to determine the hierarchy of protected rights and interests when developing domestic human rights law.**[179] Hence, there is a need for the Court to have an applicable rationale/ theoretical framework to deal with this problem. Then, what rationale can assist the Court to answer both questions asked by this section?

Squaring the ECHR with the PGC: Challenges and Suggestions

Neither the ECHR itself nor any judgement of the ECtHR provided a sufficiently clear text or rationale on reconciling competing rights and interests by applying the principle of proportionality. In this respect, the lack of such a clear criterion does not,

[178] Article 52(1) states that: 'Any limitation on the exercise of the rights and freedoms recognised by this Charter must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedom of others.'
[179] Moreham (n 76) 45-46.

at least, contradict the requirement of the PGC.[180] This is because neither the opinions of the ECtHR say anything contradicts the criterion of degrees of needfulness for action. Indeed, as we noted in the *Marper* case, the Strasburg Court declares that having a totally blanket standard is impermissible. In this regard, we must interpret the prohibition of blanket checks as the right for which more important needs for action must not be outweighed by the less important needs for action. Moreover, in terms of conditions of Article 8(2), which are all justifications in terms of human rights, it is required by the PGC that protection of rights in Article 8(2) must involve generic rights.[181] Accordingly, listed rights and interests such as the national security must be considered as being thus equitable to regard the justification of all restrictions as 'lying in the protection of the conflicting rights of others afforded by the satisfaction of such needs.'[182]

In light of this, it can be argued that the Strasburg balancing test is in line with the PGC. This is because the idea of institutional requirements to override other rights is comparable to the principle of proportionality.[183] Moreover, precautionary reasoning requires that the risk of violating the PGC is minimised. This idea is also broadly in agreement with the proportionality principle in the narrow sense (one of the three sub-principles of the proportionality principle).

4.3.4 The Added Value of the PGC

This subsection aims to present that **the criterion of degrees of needfulness for**

[180] Beyleveld and Brownsword, *Human Dignity in Bioethics and Biolaw* 85.
[181] This is because only generic rights (with a higher degree of needfulness for action) can override generic rights under the PGC.
[182] Beyleveld and Brownsword, *Human Dignity in Bioethics and Biolaw* 85.
[183] Gewirth, *Reason and Morality* 344.

action offers a coherent rationale as an assessment to reply to issues previously presented: (1) The rationale to assist the ECtHR to identify those aforementioned rights? (2) The difficulty in ascertaining exactly what local courts should be 'taking into account' when developing domestic human rights law.

The Criterion of Degrees of Needfulness for Action

It has been indicated that the generic rights/GCA are ordered according to a hierarchy arranged by the degree of their essentiality in relation to an agent's purpose-fulfilments. In this respect, basic rights are ranked at the highest level and the non-subtractive rights are more needed than the additive rights. Among and within each level of capabilities of action, moreover, there is also a hierarchy determined by the degree of their indispensability.[184]

Compared to the principle of proportionality, the operation of the criterion is able to satisfy the requirement of consistency. We can imagine the proportionality principle itself as a balance scale that might be used to determine the weight of competing rights. This balance scale, however, lacks a clear criterion to rank/ measure the weights on each side of the balance scale. To merely apply the proportionality principle is similar to use a balance scale in space. The consequence of weighing the competing rights is thus inconsistent since the weight of the rights cannot be measured/ presented: every judge/ person may weigh the objects based on their own variable and contingent perspectives. For example, under the *Golden Rule*, it depends on contingent factors about how people would like to be treated.[185] Differently situated people may have different preferences based on contingencies. Thus by

[184] Ibid 62-63. See: section 3.6.
[185] Two versions of the Golden Rule should be distinguished. Positively, an agent should treat others as one would like others to treat oneself, whereas negatively, an agent should not treat others in ways that one would not like to be treated.

putting contingent judgements on the proportionality balance scale, this can result in divergent consequences.

On the other hand, the criterion considered here acts as *the law of gravity (gravitation), which gives weight to objects according to degrees of needfulness for action*. What matters is not how people feel/ what they prefer under specific circumstances. The PGC requires, rather, agents to act in accordance with generic rights of all agents, which is a categorical imperative. Thus any agent who exercises the criterion of degrees of needfulness for action should reach the same conclusion. The criterion is meant to avoid inconsistency. This, however, leaves a question unanswered: would other criteria also be able to offer other 'laws of physics' to assist the proportionality balance scale?

Unique features of this criterion are yet to be noted and explored in depth. They will be closely related to the ideas of collective rights and Utilitarian calculating claims. The criterion of degrees of needfulness for action enters into some disputed questions (mainly from the Libertarianism) that have implications for the Utilitarian calculation. To reply to the objections, some Gewirthian claims thus need to be recalled in order to mark out the differences from the Utilitarian arguments. Let us presume, in the features addressed below, that A is more needed necessary for action than B.

1. The criterion is able to deal with the collective right or the public good.[186] It must be noted that a collective right can be also construed as an individual right. This is because by applying the PGC indirectly a collective right within a given community/ society presents a right which is designed to improve the

[186] Gewirth, *The Community of Rights* 48.

benefits of all agents in said community/ society.[187]

This characteristic must, however, be distinguished from the value of collective rights under Utilitarianism:[188]

(1) The distributive aspect of collective rights requires any legal system that indirectly applies the PGC to treat the agents affected by it *equally*.
(2) Unlike utilitarian that focus on the overall benefit/ happiness, the rights under the criterion of degrees of needfulness for action can be divided into different parts.
(3) For the criterion to apply, both A and B must amount to a generic right under the PGC thinking. The PGC focuses on the needs for agency. This differs from the Utilitarian idea that mainly concentrates on the overall happiness and painfulness.
(4) The collective interest under the PGC must be equally shared by the community/ society for *its own sake* rather than merely as a means of maximising overall utility.

Indeed, a common objection against the Utilitarian argument has been noted: since Utilitarianism holds that the higher pleasures should always be pursued in order to achieve the maximum sum of happiness, why do sometimes agents prefer lower pleasures to higher pleasures?[189] The application of the PGC is capable of responding to this objection by opening up to Utilitarian thinking, as the benefits of the rights and interests can be waived under the voluntarily condition of the PGC.

[187] Ibid 48.
[188] Ibid 48-49.
[189] Michael J. Sandel, *Justice: What's the Right Thing to Do* (Penguin Books 2010) 54-56.

2. The criterion is different from some versions of the Utilitarian theories, which hold that enlarging/ increasing the amount of A could be made by taking away by sacrificing/ diminishing of B.

   By paying attention to the sum of the satisfaction of happiness,[190] it is arguable that the Utilitarian logic, in particular Bentham's ideas, fails to respect individual rights. On the Utilitarian ground, individuals only matter 'in the sense that each person's preferences should be counted along with everyone else's.'[191] To reply to this, it might be argued that considering all things together, some extreme harm (such as torture) to individuals may not be practically applicable. However, in this regard, it must be noted that this is because, by doing so, there will be an overall negative effect, rather than because of the need to respect individual dignity.

   John S. Mill later considers that, in the long run, respecting individual liberty is the way to achieve the greatest happiness. Nevertheless, the moral basis seems not fully convincing. This is because: (i) there can be alternative routes to achieving long-term happiness; and (ii) violating individuality may not always be the wrong thing to do – if doing so can achieve long-term benefits.[192]

   On the other hand, the thinking of the PGC draws its inspiration from the Kantian theories.[193] Here, the Formula of the End in Itself has been argued as

[190] According to Jeremy Bentham, '[b]y the principle of utility is meant that principle which approves or disapproves of every action whatsoever, according to the tendency it appears to have to augment or diminish the happiness of the party whose interest is in question: or, what is the same thing in other words, to promote or to oppose that happiness.' Jeremy Bentham, *An Introduction to the Principles of Morals and Legislation* (J. H. Burns and H. L. A. Hart eds, 1970) 11-13.
[191] Sandel (n 189) 37.
[192] Ibid 50-51.
[193] Beyleveld and Brownsword, *Human Dignity in Bioethics and Biolaw* 87-110.

in agreement with the Gewirthian manner.[194] In this regard, the PGC can 'be derived from this formula merely by specifying possession of the generic needs as the necessary means of agency.'[195] Here, it must be emphasised that to possess a right to agency under the PGC is to possess a right to the *necessary* means of agency as such.

Moreover, the context of agency under the PGC does not have a tendency to encourage passive agents who depend on the agency of another. It is pointed out by Gewirth that

> [t]he rational autonomy which is the aim of the human rights involves that each person is to be a self-controlling, self-developing agent, in contrast to being a dependant, passive recipient of the agency of others. Even when the rights require positive assistance from other persons, their point is not to reinforce or increase dependence but rather to give support that enables persons to be agents…[196]

The criterion here is thus concerned with preventing violations of necessary means of agency (including *harms* consisting in removing or threatening the basic, non-subtractive, or additive rights available to all agents), rather than increasing the benefits.[197] For example, under the PGC, a provision allowing landlords to permanently seal or darken all the windows in order to *increase* the lodgers' privacy rights such as the right to be let alone, may not be allowed.

---

[194] Ibid 98.
[195] Ibid 98.
[196] Gewirth, *The Community of Rights* 52.
[197] Gewirth, *Reason and Morality* 344.

3. This criterion also differs from the Utilitarian thinking that **A might ≤ B*X**, if the scale of X is large enough (i.e., the weight of B*X can outweigh the weight of A) under the Utilitarian measurement.

   This idea seems to be in line with the cost-benefit analysis. By measuring and calculating happiness, Utilitarian thinking weighs the preferences of happiness and pain instead of judging their moral worth. On this basis, the principle of utility translates moral good into a 'common currency' of value.[198] The criterion applied by the utilitarian logic to compare competing interests is thus to compare happiness (the common currency) under the cost-benefit analysis. In terms of the common currency – the benefit/happiness – applied by the principle of utility, it is noted that Bentham 'recognizes no qualitative distinction among pleasures.'[199] It seems therefore that the level of happiness has not been distinguished and all preferences should count equally. The obvious objection with regard to this 'single currency' term is to doubt whether it is possible to do so – how to translate, for example, human life, dignity, or honour into happiness?[200]

   To justify this objection, Mill accepts that there are higher pleasures, which are more desirable and valuable than others. As regards the criterion of determining the quality of happiness/ painfulness, he suggests: '[o]f two pleasures, if there be one to which all or most all who have experience of both give a decided preference, irrespective of any feeling of moral obligation to

[198] Sandel (n 189) 41.
[199] Ibid 52, cited from John S. Mill, *Utilitarianism* (George Sher ed, first published 1861, Hackett publishing 1979).
[200] Gewirth termed this question 'the impossibility of interpersonal comparisons of utility or well-being.' Gewirth, *The Community of Rights* 50.

prefer it, that is the more desirable pleasure.'[201]

Under the PGC, the criterion of degrees of needfulness for action cannot be applied in this way. If A is more needed for action for an agent than B, A will not be overridden by B – even B is held by a large number of agents. For example, as Gewirth illustrates, the 'limits' of the application of the criterion of degrees of needfulness for action particularly concern body integrity as an essential part of the basic condition of agency.[202] Since the criterion granted by the PGC is distinguished both qualitatively and quantitatively, it is possible to avoid the above criticise in terms of the single currency (happiness).

However, it must be emphasised that to apply the PGC in society, the need of A for action may change to being less important than the need of B. Then A<B, so B can override A in competing cases.

An Example of Applying the Criterion of Degrees of Needfulness for Action

Let us see how the criterion will work by taking the *Marper* case outlined above as an example.[203]

1. Identify the rights covered by Article 8(1) of the ECHR

The Court recognises that fighting against organised crime and terrorism depends 'to a great extent on the use of modern scientific techniques of investigation and identification.'[204] Under the principle of instrumental reason, to defend the public

[201] Mill (n 199), cited from Sandel (n 189) 54.
[202] This thesis mainly focuses on human beings as the agents. The body integrity thus is a basic need. It must be noted that 'what materially instantiates the generic conditions is, to an extent, an empirical matter, being contingent upon the species of the agent.' See: Beyleveld and Brownsword, *Consent in the Law* 51-52.
[203] For similar case of the ECHR, see *Goggins and Others v The United Kingdom*.
[204] *S and Marper v UK* para 105.

good of national and social security, the instrument (storing and processing personal biometric data in the database) to exercise this interest must be granted readily.

Since there is a generic need for action, there is a positive duty bestowed upon data controllers. This is because the PGC requires agents to assist those agents to secure the generic conditions for action when they cannot do so by their own unaided efforts and comparable cost if they so wish. Therefore, the positive duty imposed on the data controllers implies a duty to provide and participate in a well-designed and well-maintained database in order to prevent generic harm to other agents. However, the benefits of storing and processing personal biometric data, which is a crucial instrument to protect national and societal security (collectively as well as individually), might interfere with other related generic rights – such as the right to privacy and data protection.

2. Value the relative rights in terms of the generic conditions for action

A preliminary question must be asked before comparing the rights covered by Article 8(1) of the ECHR, regarding whether a broad or narrow conception of privacy should be recognised. The English courts, on one hand, in some cases apply a narrow concept of privacy.[205] On the other hand, as previously discussed, the ECtHR and some English judgments[206] do accept a broader conception of privacy. So, how do the Gewirthian scholars answer this question?

A generic right is to be granted to any generic condition of action on the PGC ground. In this regard, undoubtedly, 'there are the generic conditions of action that do

[205] *R v Chief Constable of South Yorkshire* [2004] UKHL 39 paras 26, 28. See also: *Durant v Financial Services Authority* [2003] EWCA Civ 1746; *R v Department of Health ex p. Source Informatics* [2001] QB 424.
[206] E.g. *Campbell v. MGN* [2004] UKHL 22.

not find expression in the other rights of the ECHR.'[207] As the definition of the right to privacy remains vague, this is particularly true with respect to Article 8(1) of the ECHR. Moreover, since there are generic conditions for action, whether they find expression in the other rights of the ECHR or not, *there must also be the right to these generic needs of agency*. It is therefore better for human rights instruments to accept a broader conception of privacy. This is in agreement with the opinion of the ECtHR. Hence, it is suggested that the dispute in the *Marper* case poses a threat to the right to privacy and Article 8(1) is involved.

3. Decide which generic rights take precedence over the other generic rights

On the basis of the criterion of degrees of needfulness for action, the values of storing and processing personal biometric data **CANNOT** override other types of the right to privacy in **ALL** cases of conflict.[208] The right to benefit from technological advances (the retention of personal biometric data values)[209] is **NOT** more important than **ALL** other fundamental rights and freedoms protected in the data protection law regime.[210] This is simply because that it is not an absolute right under the PGC.

In the *Marper* case, several rights are not less important than the retention values: the interest of preventing the risk of stigmatisation,[211] for example, can be viewed at least as a non-subtractive need. On the other hand, *without proportionate limitations*, the biometric database cannot be viewed as a basic need since it is not the only or an

[207] Beyleveld and Pattinson, 'Moral Interests, Privacy, and Medical Research' 50.
[208] For similar discussions, see: Deryck Beyleveld, 'Data Protection and Genetics: Medical Research and the Public Good' (2007) 18 King's Law Journal287, and Beyleveld and Pattinson, 'Moral Interests, Privacy, and Medical Research' 54-56.
[209] See section 6.2.
[210] Article 1.1 of the Data Protection Directive states that '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.' Thus, ALL of the fundamental rights and freedoms of natural persons with respect to the processing of personal data are under the scope of data protection.
[211] *S and Marper v UK* paras 122-123.

essential means leading to the *very possibility* of achieving the purpose which can at the same time minimise the risk of violating the PGC. The other GCA under the scope of the right to privacy, for example the need to protect minors' mental equilibrium,[212] which can be viewed as either a basic need or a non-subtractive need, may also override the additive need. Moreover, it should be noted that not all biometric databases are well-structured and safe. It has been previously argued that there are a number of risks regarding safety issues in applying biometric technologies. Unsafely built and managed biometric databases can lead to serious violations of both human rights and generic needs.

However, there is a question to be considered: under the PGC, can a majority, however big, of the lower degree of needfulness for the GCA override an individual's higher needfulness for the GCA? The answer is No. This is because, as we have seen, it is NOT 'of whether such interference will or will not promote the general welfare but rather of *the equality of generic rights*.'[213] (emphasis added)

With regard to Lord Steyn's opinion that 'judicial decisions can be made, when the need arises, to ensure compatibility with the ECHR', it must be emphasised that '[s]ince the PGC is categorically binding, it can never be justifiable to run the risk of violating it where this can be avoided.'[214] Hence, the risk of violating the PGC must be minimised *if at all possible*. Under the precautionary reasoning, the 'wait and see' policy held by the House of Lord thus runs the risk of violating the PGC.

Overall, the blanket permission for such databases or the idea that 'the more complete the database, the better the chance of detecting criminals' suggested by Lord

[212] Ibid para 124.
[213] Gewirth, *Reason and Morality* 326.
[214] Pattinson (n 47) 599.

Brown is unable to pass the tests that underlies the PGC. Considering the broad concept of privacy, it might be wrong to consider privacy/ data protection values and other values as 'belonging to two mutually exclusive sets.'[215] The conflict of the mentioned competing rights, i.e., applying new technologies as a regulatory instrument might be solved by, for example, obtaining explicit consent or new technology itself.[216] A concrete example is offered by Privacy Enhancing Technologies (PETs).[217] Indeed, the use of modern scientific techniques of investigation and identification to fight against threats to the quality of private life, arguably, can be considered as a privacy value. We shall revisit and expand this idea in Chapter 7.

4.4 Summary

This chapter has offered a brief overview of the concept of privacy. From the analysis set out we have seen that the broad concept of privacy should be taken as the way of interpreting Article 8 in order to render it consistent with the PGC's requirements. We have also seen that the added value of the PGC is to offer a theoretical framework for identifying the generic rights. By justifying the PGC as the basic principle for human rights, moreover, this analysis has claimed that the PGC can assist in the reconciliation of conflicts of rights and interests.

So far the chapter has shown how to specifically apply the PGC to the issues

[215] Beyleveld, 'Data Protection and Genetics: Medical Research and the Public Good' 287.
[216] Argued by Gewitrh, only in some particular extreme occasions, 'when a necessary-procedure justification based consequences of the method of consent conflict with a dynamic-instrumental justification based basic harms done by polices,' the latter rights/interests overrides the former. Gewirth, *Reason and Morality* 319-322.
[217] See: section 7.2.

considered in this thesis. In the following chapters, we shall move onto spelling out the European and Formosan data protection positions and identifying issues for the PGC.

Chapter 5

Data Protection Legislation in Europe and Taiwan

5.1 Introduction

In the context of global data protection regulatory frameworks, there are two different models, namely the American model (freedom of information model) and the European model (personal data protection model).[1] As Francesca Bignami states,

> [i]n the European Union, privacy is essential to protecting citizens from oppression by the government and market actors and preserving their dignity in the face of opposing social and political forces. In the United States, privacy is secondary.[2]

This partly explains the choice of studying the European model as part of this research on data protection regimes. Moreover, both the first data protection act in the world[3] and the most influential data protection mechanism, i.e., the Data Protection Directive, come from Europe. It is, therefore, necessary for any researcher who is interested in data protection regulatory frameworks to examine the European context. On the other hand, as regards the Taiwanese part, the Computer-Processed Personal Data Protection Law (CPDPL)[4] owed its genesis to the Guidelines on the Protection of

---

[1] Dorothee Heisenberg, *Negotiating Privacy: The European Union, The United States, and Personal Data Protection* (Lynne Rienner Publisher 2005) 13. Also, Adam D. Moore, 'Owning Genetic Information and Gene Enhancement Techniques: Why Privacy and Property May Undermine Social Control of the Human Genome' (2000) 14 Bioethics 108-109.

[2] Francesca Bignami, 'Transgovernmental Networks vs. Democracy: The case of the European Information Privacy Network' (2005) 26 MICH J INT'L L 807. See also, Joel Reidenberg, 'Setting Standards for Fair Information Practice in the U.S. Private Sector' (1995) 80 IOWA L REV 497, 500.

[3] In 1970, the Data Protection Act of the Land of Hessen, German, was the first data protection act in the world. See: ePractice.eu, 'eGovernment Factsheet - Germany - Legal framework' (2010) <http://www.epractice.eu/en/document/288243> accessed May 25 2010.

[4] It was promulgated by Presidential Decree Ref. No. ROC-President-(I)-Yi-5960, 11 August, 1995. A revision of the CPDPL, which has been renamed as the "Personal Data Protection Law," passed preliminary review in the Legislative Yuan on April 18, 2010.

Privacy and Transborder Flows of Personal Data (hereinafter, OECD Guidelines)[5] and the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (hereinafter, Data Protection Convention).[6] In order to research Taiwanese data protection legislation it is essential to look at the European perspective.

This chapter is structured as follows: sections 5.2 and 5.3 survey data protection laws at the European and Formosan level respectively; section 5.4 investigates concepts of the right to privacy in Taiwan; section 5.5, building on the essential knowledge on the legislation and concepts of data protection law and concepts of privacy in the two legal regimes, identifies issues for the later evaluations.

5.2 Data Protection Law and New Technologies: European Context

5.2.1 Data Protection in European Law: the Data Protection Directive as the Main Regulatory Instrument in Europe

5.2.1.1 The Historical Track of Data Protection Law: a Complex Nature of Primary Legislative Sources

5.2.1.1.1 International Instruments

- **International Human Rights Instruments and Privacy**

[5] It was adopted on 23 September 1980. Available at: < http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html#part2> accessed 28 February, 2010.
[6] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, ETS no. 108, 1981.

The EU[7] is under an obligation to uphold international law when exercising its powers.[8] Article 12 of the Universal Declaration of Human Rights (UDHR)[9] states that:

> No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.

This principle is echoed in Article 17 of the International Covenant on Civil and Political Rights (ICCPR).[10] The protection of the right to private life in these two core international human rights instruments is also invoked in regional human rights instruments. The American Convention on Human Rights,[11] for example, provides it in Article 11. As regards the European human rights framework, it is provided in Article 8 of the ECHR. Differently from other international human rights instruments, Article 8(2) introduces relevant elements that need to be satisfied in order to for assess interference.

Despite offering certain considerations on the right to privacy, the above materials remain vague with regards to data protection. In relation to the ECHR, for example, although case law judgements of the ECtHR could contribute to part of core data protection principles, Karanja observes that '[w]hen such principles are given

---

[7] The Treaty of Lisbon amending the Treaty on European Union (TEU) and the Treaty establishing the European Community has entered into force on 1 December, 2009. Consequently, as from that date, references to the EC shall be read as the EU.

[8] Case C-286/90 *Anklagemyndigheden v. Poulsen and Diva Navigation* [1992] ECR I-6019, para 9. Paul Craig and Gráinne De Búrca, *EU Law: Text, Cases and Materials* (5th edn, OUP 2011) 341.

[9] It was proclaimed by the General Assembly of the United Nations on 10th December 1948. Available at: < http://www.un.org/en/documents/udhr/> accessed 28 February, 2010.

[10] It was adopted and opened for signature, ratification and accession by General Assembly resolution 2200A (XXI) of 16 December 1966 (entry into force 23 March 1976, in accordance with Article 49). Available at: < http://www2.ohchr.org/english/law/ccpr.htm> accessed 28 February, 2010.

[11] It was adopted on 22nd November, 1969 at San Jose, Costa Rica (entry into force 18 July 1978, in accordance with Article 74.2). It mentions the Universal Declaration of Human Rights in its preamble as well.

weight, it is only incidental rather than intended'.[12] Consequently, he argues that those decisions would be unable to assess interferences through 'a consistent set of principles.'[13] Indeed, the idea and concepts of privacy were at the initial stage and rather undeveloped at the time when these key instruments were introduced. When 'Information, Communication and Technology (ICT)'[14] have been involved, unsurprisingly, the aforementioned (vague) privacy protections, cannot meet the new demands of the communication society and the information era in 1970's.

- **International Data Protection Instruments**

The UN subsequently issued the United Nations guidelines concerning Computerized Personal Data Files.[15] However, this has only had a relatively limited impact on the worldwide data protection law regime.[16]

Eight core data protection principles of the OECD Guidelines issued by the Organisation for Economic Cooperation and Development (OECD) aim to harmonise data protection legislation for economic reasons and map out the key principles of data protection.[17] This has had a worldwide impact on the later development of data

[12] Ibid.
[13] Ibid.
[14] The RAND report of Review of the European Data Protection Directive describes the appearance ICT in 1970s resulted as 'increased the risk of personal data being abused and created concern that there would be a need for regulation to ensure that individuals remained adequately protected.' See: Neil Robinson and others, *Review of the European Data Protection Directive* (Technical Report, 2009) 6. It is also addressed by Ronald et al. that certain legislation and case law responded to the need for regulation on ICTs, such as large-scale processing of personal data in 1980s and internet in 1990s. According to their opinion, those legislation and case law were, however, not sufficient. See: Ronald Leenes, Bert-Jaap Koops and Paul de Hert, 'Introduction' in Ronald Leenes and others (eds), *Constitutional rights and new technologies: a comparative study* (T.M.C.Asser Press 2008) 1.
[15] It was adopted by the General Assembly on 14 December 1990.
[16] *Stephen Kabera Karanja, Transparency and Proportionality in the Schengen Information System and Border Control Co-operation (Martinus Nijhoff Publishers 2008)* 124. Moreover, it is also suggested by Lee Bygrave that in Scandinavia the aforementioned UN guidelines has indeed been overlooked. Lee A. Bygrave, *Data Proteciton Law: Approaching Its Rationale, Logic and Limits* (Kluwer Law International 2002) 33.
[17] Paragraph 6 of the Guidelines: These Guidelines should be regarded as minimum standards which are capable of being supplemented by additional measures for the protection of privacy and individual liberties.

protection legal regimes, particularly in the OECD areas: Europe, North America, and East Asia. Examples can be found at national level in the United States, Australia, New Zealand, and South Korea.[18] Furthermore, the Asia-Pacific Economic Cooperation (APEC) Ministers endorse the APEC Privacy Framework,[19] which agrees that the OECD Guidelines represent the international consensus on the protection of informational privacy.[20]

According to Article 216(2) TFEU,[21] if international agreements are entered into by the EU, those agreements are held to be an integral part of the EU legal order.[22] However, it should be noted that the EU is not a party to any of these aforementioned international instruments and the Union itself is not directly bound by them (although individual member states that have ratified these instruments will be).

5.2.1.1.2 European Data Protection Legal Framework

The Data Protection Convention is undeniably one of the key reference points in Europe for this topic. For instance, the scope of the Schengen Convention relies on the Data Protection Convention as a supplementary source along with national legislation.[23] After the Data Protection Convention, several relevant normative

[18] Daniel J. Solove and Paul M. Schwartz, *Informational Privacy Law* (3 edn, Aspen Publishers 2009) 998.
[19] It was endorsed by the APEC Ministers in 16th APEC Ministerial Meeting, Santiago, Chile, 17-18 November 2004.
[20] The APEC Privacy Framework states that it is 'consistent with the core values of' the OECD Guidelines' and 'reaffirms the value of privacy to individuals and to the information society.' Citation 1, paragraph 5 of the APEC Privacy Framework. Part III of the APEC Privacy Framework therefore reaffirms those eight key principles.
[21] I.e., Article 188L, which is the article number used in the text of the Lisbon Treaty.
[22] Case 181/73 *Haegeman v Belgium* [1974] ECR 449, para. 5. Under this circumstance, the member states are bound by international agreements as a result of their duties under Community law, not international law. See Case C-239/03 *Commission v. France (Etang de Berre)* [2004] ECR I-9325, para 26. Also, Craig and Búrca (n 8) 344.
[23] Karanja (n 16) 128.

documents have been passed in order to elaborate its content. This includes the 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[24] and related regulations and recommendations.

The principles stated by both the OECD Guidelines (paragraph 6) and the Data Protection Convention (Article 11) are to be considered as minimum standards. It has been observed in a RAND report,[25] however, that there was little harmonisation between these two regulatory texts before the introduction of the Data Protection Directive. This might be explained by the nature of these two instruments: while one is introduced for economic reasons, the other's purpose is to protect fundamental rights.[26] The variation of regulatory instruments at national level led to a barrier to the fluent exchange of personal data which is contained in both of the private business sector and the public sector. Influencing every pillar of the EU, therefore, the need to establish a foundation for a proper harmonisation, particularly in terms of the first pillar, was then reflected in the Data Protection Directive.[27]

After the introduction of the Data Protection Directive, the EU then issued several related instruments concerning different sectors for processing personal data. With respect to electronic communications, particularly the internet, for example, Directive 2002/58/EC was issued in 2002.[28] Moreover, in terms of retention of

[24] ETS no. 181. It was adopted in Strasbourg, 2001. This additional protocol mainly deals with issues regarding supervisory authorities (Article 1) and transborder flows of personal data to a recipient which is not subject to the jurisdiction of a party to the Convention (Article 2).
[25] Robinson and others (n 14).
[26] It is noted that if one reads these two values separately, they are prone to coming into conflict. To ensure a more harmonised application of the law, a broad concept of privacy should be accepted.
[27] This is addressed through the Recitals 7-10 of the Data Protection Directive. The main content of the Data Protection Directive will be described in the later section of this chapter.
[28] 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 (Directive on privacy and electronic communications), OJ L 201, 31/07/2002 P. 0037 – 0047.

information concerns in public communication networks or electronic communications services, the EU issued Directive 2006/24/EC (Data Retention Directive) [29] which amended Directive 2002/58/EC. The Data Retention Directive specifically applies to data protection in law enforcement activities.[30] The EU then issued Directive 2009/136/EC on universal service and users' rights relating to electronic communications networks and services amending Directive 2002/58/EC.[31] This Directive draws attention by requiring informed consent before information is retained or accessed in the users' terminal device under Article 5.3.[32]

There was no pan-European general human rights instrument separating the right to private life and data protection in the last century. In 2000, this changed. Article 7 of the Charter of Fundamental Rights of the European Union provides the right to private life as Article 8(1) of the ECHR. Meanwhile, Article 8 of the Charter states that:

1. Everyone has the right to the protection of personal data concerning him or her.
2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.

[29] 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 L 105, 13/04/2006 P. 0054 – 0063.
[30] Francesca Bignami, 'Privacy and Law Enforcement in the European Union: The Data Retention Directive' (2007) 8 Chicago Journal of International Law 233-255.
[31] 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, P. 0011-0036.
[32] This article has profound impact on the usage of cookies on the internet. For detailed discussion and opinions in relation to the consent exemption, see: Article 29 Data Protection Working Party, *Opinion 04/2012 on Cookie Consent Exemption* (No 00879/12/EN, WP194, 2012).

3. Compliance with these rules shall be subject to control by an independent authority.

Paragraph 2 of the article clearly points out *some* key data protection principles and general rules on the lawfulness of processing of personal data. Moreover, paragraph 3 introduces the framework of independent authority to control and monitor this new type of right. The rights protected by Articles 7 and 8 of the Charter have been recognised by Article 1.8) of the Lisbon Treaty. Such a distinction between the right to privacy and data protection can also be found in the Convention for the Protection of Human Rights and Dignity of the Human Being with regard to the Application of Biology and Medicine (hereinafter termed in 'the Convention on Human Rights and Biomedicine').[33]

Overall, the Data Protection Directive is a significant milestone. This is because:

1. Before the Directive, there was no effective and specific international instrument which focused on interferences through the processing of personal data;
2. The Directive considers both the human rights approach and the economic approach from which it aims to harmonise data protection legislation of

[33] ETS no. 164, 1997. See Articles 10 and 26.1. It should be noted that the Convention on Human Rights and Biomedicine has not been signed and ratified by all EU members, e.g, Germany, Ireland, Italy, Luxembourg, Netherlands, and United Kingdom. Moreover, there are also declarations and reservations with respect to this Convention. With reference to Article 10 at issue, for example, Denmark makes a reservation that '[a]ccording to this provision, all persons are entitled to know any information collected about his or her health. However, the wishes of individuals not to be so informed shall be observed.' This has been criticised as doing 'little more than pay lip-service to these measures, and continue to implement domestic laws in flagrant breach of their provisions.' See: Kenyon Mason and Graeme Laurie, *Mason and McCall Smith's Law and Medical Ethics* (8th edn, OUP 2011) 42. For the latest update of the Convention, see: Council of Europe, 'List of declarations made with respect to treaty No. 164' (*Council of Europe*,, 2012) <http://conventions.coe.int/Treaty/Commun/ListeDeclarations.asp?NT=164&CM=&DF=&CL=ENG&VL=1> accessed 15 May 2012, and Council of Europe, 'Chart of Signatures and Ratifications (Convention for the protection of Human Rights and Dignity of the Human Being with regard to the Application of Biology and Medicine: Convention on Human Rights and Biomedicine CETS No.: 164)' (*Council of Europe*,, 2012) <http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=164&CL=ENG> accessed 5 May 2012.

states (Article 1 of the Directive);[34] and

3. The Directive, which is a main regulatory instrument in Europe, extends its influence *globally* (Article 25 of the Directive),

5.2.1.2 The Content of the Directive: An Interpretive Description

This section provides an overview on the Data Protection Directive and related provisions, which are the main data protection regulatory instruments in Europe.[35] It should be noted that the intention of this section is to outline the provision of the Directive with the processing of personal data for biometric and RFID usages in this thesis, rather than to provide a detailed overview of the Directive.

5.2.1.2.1 Purpose and objective

Article 1 states the objective of the Data Protection Directive and is a key to the interpretation of all of the later elements of the Directive. At the pre-Lisbon stage, according to Article 1.1, *for the purpose of a harmonised manner of the internal market*, the Data Protection Directive aims to safeguard fundamental rights and freedoms of natural persons, *especially* the right to privacy, in order to enable the free flow of personal data from one EU Member State to another. In sum, under the Data Protection Directive, data protection covers the protection of *all* fundamental rights

[34] However, this does not mean that the Directive considers the balance between these two perspectives. Also, Deryck Beyleveld, 'An Overview of Directive 95/46/EC in Relation to Medical Research' in Deryck Beyleveld and others (eds), *The Data Protection Directive and Medicial Research Across Europe* (Ashgate Publishing 2004) 6-7.

[35] The member states of the EU were obliged to issue the national legislation that give effects to the Directive. In addition, three non-EU members of the European Economic Area (EEA), including Iceland, Liechtenstein and Norway), have also ratified the Data Protection Directive.

and freedoms regarding personal data, and in particular (but *not* only) the right to privacy.[36]

Three points need to be noted. Firstly, the Directive does not give a clear indication as to whether or not it concerns itself with striking a balance between single market objectives and the protection of fundamental rights and freedoms. However, before the Lisbon Treaty in 2009, The Directive (Article 1.2) shall not be interpreted as the purpose of the Directive is to essentially strike a balance between fundamental rights and internal market. This is because the central purpose of the Directive is to enable the free flow of personal data between the EU members.[37] At the post-Lisbon stage, nevertheless, as required by Article 6 TEU, human rights provisions in the EU Charter of Fundamental Rights have been upgraded as possessing the same binding legal effect as the Treaties. Yet, as Craig and De Búrca comment,[38]

> …the legacy of the EEC's roots in the common market project remains significant since, despite its constantly changing and expanding nature, the EU's dominant focus remains economic, and the debate over the appropriate scope of its human rights role remains even after the important changes introduced by the Lisbon Treaty.

In this regard, it has been suggested that this is best viewed as 'internal' to the activity of the protection of fundamental rights and freedoms.[39] Indeed, 'the economic well-being of a country' in relation to interests brought by the free flow of personal data between the EU members *can also be regarded as a type of interest concerning private life under the heading of the right to private life in Article 8(1),* or *the public*

[36] It is further pointed out by Beyleveld that the Directive is often misunderstood as the 'Privacy Directive'. See: Beyleveld (n 34) 6.
[37] Ibid 6.
[38] Craig and Búrca (n 8) 364.
[39] Beyleveld (n 34) 7.

interest laid down by Article 8(2). With the idea of the internal activity of protecting the right to private life, it is not necessary to have a conflict between the protection of fundamental rights and freedoms as such and any other factors (e.g., the free movement of personal data between the EU members). To view this matter internally, therefore, can avoid the unnecessarily and inconsistency with the notion of integrity of protecting fundamental rights and freedoms. [40] This is consistent with the broad concept of privacy and remains valid after the introduction of the Lisbon Treaty. Moreover, this idea is even more crucial with reference to rapid technological developments and globalisation which require 'further facilitat[ion of] the free flow of data within the Union and the transfer to third countries and international organisations, while ensuring a high level of the protection of personal data.'[41]

Secondly, to interpret the fundamental rights and freedoms set out in Article 1, the rights recognised in the ECHR, which have been treated by the ECJ as a 'special source of inspiration' for EU human rights principles[42] and required by Article 6(2) TEU to accede to the ECHR, must be taken into account. Lastly, as regards to the principles of fundamental rights and freedoms, which have been clarified by the ECJ to view the Charter as the principle basis,[43] Recital 11 gives substance to and amplifies those contained in the Data Protection Convention.

---

[40] Ibid. This is in line with the co-operative model in Chapter 7.

[41] European Commission, '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)' (2012) <http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf> accessed 30 Janurary 2012, Recital 5. In the 2012 EU General Data Protection Regulation, it is stated in Article 1(3) that 'The free movement of personal data within the Union shall neither be restricted nor prohibited for reasons connected with the protection of individuals with regard to the processing of personal data.'

[42] Craig and Búrca (n 8) 362.

[43] Ibid 362. It should be noted, however, the UK, Poland, and the Czech Republic negotiated a protocol to the Lisbon Treaty with respect to the impact of the Charter.

5.2.1.2.2 Definition and Scope

Article 2(a) sets out that if an identifiable person can be identified 'directly or indirectly', then this linkable data is personal data. In this respect, personal data is not within the definition of anonymisation if there is any possibility that *anyone could link* the datasets through reasonable methods.[44] It is suggested that these reasonable methods are those that do not consume disproportionate time, energy or financial means.[45]

The definition and scope of the 'relevant filing system' under Recital 27, Articles 2(c) and 3(1) are also debateable. Core characteristics of relevant filing systems include: (1) the structuring by reference to individuals; and (2) the ready accessibility of certain specific information. The UK courts have interpreted this by adopting a narrow interpretation in the *Durant* case.[46] In this case it was ruled that two conditions must be satisfied in order to determine whether information 'relates to' an individual: (1) 'whether the information is biographical in a significant sense'; and (2) the information 'should have the putative data subject as its focus rather than some other person with whom he may have been involved or some transaction or event in which he may have figured or have had an interest'.[47] Auld LJ stated that 'either on the issue as to whether a document contains "personal data" or as to whether it is part

[44] Graeme Laurie and Nayha Sethi, 'Information Governance of Use of Patient Data in Medical Research in Scotland: Current and Future Scenarios' (*Scottish Health Informatics Programme (SHIP)*) <http://www.scot-ship.ac.uk/sites/default/files/Reports/Scoping_Report_Final_August_2010.pdf> accessed 6 August 2011 at 27. See also, Deryck Beyleveld, 'Data Protection and Genetics: Medical Research and the Public Good' (2007) 18 King's Law Journal 280-283.

[45] For discussion in relation to applications of anonymisation, see section 7.2.2.

[46] *Durant v Financial Services Authority* [2003] EWCA Civ 1746. For the UK Information Commissioner Office's viewpoint toward the *Durant* Case, see: Information Commissioner Office, 'The 'Durant' Case and Its Impact on the Interpretation of the Data Protection Act 1998' <http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/the_durant_case_and_its_impact_on_the_interpretation_of_the_data_protection_act.pdf> accessed 9 June 2011, <http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/the_durant_case_and_its_impact_on_the_interpretation_of_the_data_protection_act.pdf> accessed 24 April, 2010.

[47] *Durant* para 28.

of a "relevant filing system", the mere fact that a document is retrievable by reference to his (Mr Durant's) name does not entitle him to a copy of it under the Act'[48] – even though his name was shown on the file.

However, it should be noted that later cases in other domestic courts ruled in the opposite direction.[49] Therefore, the *Durant* case must be treated carefully since it 'would be unwise to assume that the *Durant* interpretation would be followed by other EU Member States or by the ECJ.'[50]

5.2.1.2.3 Data Protection Principles

The principle-based framework provides Member States certain margin of appreciation in implementing essential measures whilst taking into account local differences and specific needs.[51]

Data Protection Directive	**Data Protection Convention**	**The OECD Guidelines**
Principles relating data quality (Art. 6): 5 principles of data protection (see below)	Quality of data (Art. 5)	Data Quality Principle
		Purpose Specification Principle
		Use Limitation Principle
Criteria for legitimacy (Art. 7)		Collection Limitation Principle

[48] Ibid para 30.
[49] *R v Rooney* [2006] EWCA Crim 1841. Also, *Dexia Bank Nederland* Case, Hoge Raad, 29 juni 2007, LJN AZ 4664. The *Dexia* Case points out that the right of access should be interpreted in a broader way, which includes a right to copy documents for a customer from a bank. See: Sjaak Nouwt, 'Towards a Common European Approach to Data Protection: A Critical Analysis of Data Protection Perspectives of the Council of Europe and the European Union' in Serge Gutwith and others (eds), *Reinventing Data Protection?* (Springer 2009) 283-284.
[50] Beyleveld, 'Data Protection and Genetics: Medical Research and the Public Good' 280.
[51] Robinson and others (n 14) 24.

Confidentiality and security of processing (Arts. 16-17)	Data Security (Art. 7)	Security Safeguards Principle
Right to information (Arts. 10-11)	Right to establish the existence of personal data (Art. 8(a))	Openness Principle
Right to access (Art. 12)	Right to access (Arts. 8(b)-(c))	Individual Participation Principle
Remedies and liability (Art. 22-23), Sanctions (Art. 24)	Right to have a remedy (Art. 8(d))	Accountability Principle

Table 5.1: General rules on the lawfulness of the processing of personal data in Europe

Article 6 includes five basic principles relating to data quality: personal data must be:

1. processed fairly and lawfully;
2. 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;
3. adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed;
4. accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified;
5. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed. Member States shall lay down appropriate

safeguards for personal data stored for longer periods for historical, statistical or scientific use.

The 1st principle of processing personal data fairly and lawfully can be read in either a broad or a narrow way.[52] The former indicates that, in order to obey this principle, 'all the requirements of the Directive imposed on processing must be complied with.' [53] This covers the whole set of rules on the lawfulness of processing personal data (Articles 7-21), including the other four principles of data protection. To read it narrowly, on the other hand, according to Recitals 30-36, only Articles 7-8 are covered. As regards the fair processing, the right to information (Articles 10-11) is related to the 1st principle by Recital 38.[54]

- **Consent in the Data Protection Principles when Processing Sensitive Personal Data**

Due to its vague provision on the legitimacy principle provided in Article 7, it has been argued that 'satisfaction of the conditions laid down by Articles 7 and 8(2) in way that do not involve the consent of the data subject at least implicitly requires the obtaining of consent to be impracticable, etc.' [55] To explain this briefly, when processing sensitive personal data,[56]

(1) Article 7 applies to all personal data; therefore, at least one condition from Article 7 as well as one condition form Article 8 will be met. Meanwhile,
(2) meeting any of the conditions of the Article 8 will automatically meet at least one condition of Article 7. For instance, meeting the condition of necessity for

[52] Beyleveld, 'An Overview of Directive 95/46/EC in Relation to Medical Research' 9.
[53] Ibid.
[54] Ibid.
[55] Ibid 12.
[56] Ibid 11-12.

the purpose of carrying out the obligations as it is authorised by national law providing for adequate safeguards will also meet the condition of Article 7(c). However,

(3) the ECtHR's opinion points out that processing sensitive data without consent is an interference to the right to private life under Article 8 of the ECHR.[57]

(4) Before the Lisbon Treaty, the ECJ took the decisions of the ECtHR seriously although it was not legally bound by them. At post-Lisbon stage, although the ECJ kept the attitude to maintain its autonomy after the accession by the EU to the ECHR, the relationship between the Strasburg and Luxembourg Courts remains mutually constructive.[58] Therefore,

(5) In the light of the exemptions in Article 8(2) of the ECHR, conditions in Article 8(2) and Article 7 are *not* entirely open alternatives. Satisfaction of the conditions laid down by Articles 7 and 8(2) of the Directive in way that do not involve the consent of the data subject requires the obtaining of consent to be impracticable.

Therefore, it is arguable that without explicit provision in the Data Protection Directive, consent should still play a key role when processing sensitive personal data such as biometric data. Furthermore, when assessing the exemptions from consent and its components, both the proportionality principle and the legitimacy principle should be genuinely considered.[59]

- **Proportionality in the Data Protection Principles**

The principle of proportionality is provided *mostly* to evaluate the balance struck

[57] *MS v Sweden* (1999) 28 EHRR 313, paras. 34-35.
[58] Craig and Búrca (n 8) 406.
[59] See: Beyleveld, 'Data Protection and Genetics: Medical Research and the Public Good' 285.

by EU/national authorities between competing interests. It should be noted that, however, since the Data Protection Directive applications in Member States do not limit the data controller as merely for national authorities, there are chances to apply the principle horizontally as well.

When applying the principle of proportionality to data protection, it should be noted that according to Article 7, either consent (Article 7(a)) or the proportionality principle (Articles 7(b)-(f)) should be considered as permitting to process personal data. It has been argued that despite the fact that DPAs in Member States seem to 'regard consent as weaker than the principle of proportionality' in biometric field in order to 'ensure a stronger level of protection biometric data,' it would be 'quiet dangerous to assume this.'[60]

- **Data Controller's Duties: Transparency Demands/ Data Subject's Rights: Information Rights**

Transparency demands in Articles 10-11 should play a core role in the Data Protection Directive (in fact, in all data protection instruments). The Directive refers Articles 10-11 as duties of the controller, not as rights of the data subject.[61] From a logical point of view, it can be considered loosely as the data subject's right. However, it must be emphasised that to regulate in this way should be considered as putting more stress on information transparency than describing it as a sort of right bestowed upon the data subjects. To exercise consent, which is of central importance when processing sensitive data and has been emphasised by the ECtHR, relevant information must be informed first.[62] Meanwhile, the transparent demands of the data

[60] Yue Liu, 'The Principle of Proportionality in Biometrics: Cases Studies from Norway' (2009) 25 Computer Law & Security Review 237-250.
[61] Beyleveld, 'An Overview of Directive 95/46/EC in Relation to Medical Research' 12.
[62] See: Beyleveld, 'The Duty to Provide Informaiton to the Data Subject: Articles 10 and 11 of

controllers are also essential to exercise information rights provided in Article 12 and Recitals 41-42 (right to access).

Moreover, Articles 10-11 and Recitals 38-39 request the data controller to provide involving personal data to the data subject and meet the principle of fair and lawful processing under Article 6. The principle of proportionality, particularly when assessing the exemptions addressed in Articles 11(2) and 13, must therefore be considered.

5.2.1.2.4 Institutional Frameworks

- **Supervisory Authorities at National Level**

Article 28 requires Member States to provide at least one[63] *independent* (Recital 62) public authority which is responsible for the application within its territory of the adopted provisions. The missions of these public supervisory authorities can be understood in three different roles:

1. As the ***promoter*** of the Data Protection Directive, a supervisory authority needs to take the promotion of the public awareness of data protection into consideration. In pursuit of the goal, Article 28(5) requires that it must draw up a public report on its activities at regular intervals.
2. As the ***guardian*** of the Data Protection Directive, a supervisory authority is responsible for consulting (Article 28(2)) and monitoring (Article 28(1)) the application of domestic legislation. To comply with this purpose, it should not

Directive 95/46/EC' 69-87.

[63] In the UK, there is an Information Commissioner Office and a Scottish Information Commissioner.

only cooperate in a vertical axis to monitor the applications within one state/area, but also co-operate with the supervisory authorities in other Member States horizontally (Article 28(6)).

3. As the ***defender*** of the Data Protection Directive, it should be able to defend individuals against the excessive power exercised by their governments. This is especially important in a trend of authoritarian states which increasingly extends beyond the traditional police tasks.[64] In this regard, the authority in charge must be given investigative powers, effective powers of intervention, and the power to engage in legal proceedings (Article 28(3)). Moreover, it must be able to hear claims lodged by any data subject (including associations representing the data subject) and for checks on the lawfulness of data processing lodged by any person when the national provisions adopted pursuant to Article 13 of this Directive apply (Article 28(4)). Moreover, the outcome of the claims should be made public or accessible to the individuals affected.

Considering the importance of all these missions, consequently, the supervisory authorities must not only be independent, but also organised professionally and in light of the aims of such a position.

- **The Article 29 Working Party**

The Article 29 Working Party (WP29), which plays its independent role at EU level, was set up to provide advisory suggestions and reviews. The main target of the WP29 is to harmonise data protection principles by contributing to the uniform application of the national measures adopted under the Directive (Article 30(1)(a))

[64] Foundation for Information Policy Research, *Paper No. 5: Conclusions & Policy Implications* (UK Information Commissioner Study Project: Privacy & Law Enforcement, 2004).

and to enable an internal market for personal data. Whenever the WP29 notices divergences likely to affect individuals regarding the processing of personal data in the EU, according to Article 30.2 of the Directive, it shall inform its professional opinions and recommendations to the Commission which is to be assisted by a Committee referred to in Article 31.

5.2.1.3 The Relationships between the Data Protection Directive, the ECHR and the Data Protection Convention

Perhaps the description given in a report for the UK information commissioner study project of its observation can convincingly present the complex nature of data protection legal framework at the European level: '…the Data Protection Directive builds on the Data Protection Convention in order to secure to individuals the protection of Art. 8 of the ECHR…'[65] The first dimension of the relationship between the ECHR and the Data Protection Convention has already been addressed in 5.2.1.1.2. The other two dimensions will be discussed in this subsection.

5.2.1.3.1 The Data Protection Directive and the ECHR

Although the two systems of law in the EU and the CoE are institutionally and legally separate, the Data Protection Directive, which is applied in the EU Member States as a main regulatory instrument in Europe, gives effect to fundamental rights and freedoms protected in the ECHR.

[65] Foundation for Information Policy Research, *Paper No. 4: The Legal Framework: an Analysis of the "Constitutional" European Approach to Issues of Data Protection and Law Enforcement* (UK Information Commissioner Study Project: Privacy & Law Enforcement, 2004).

Before the Treaty of Lisbon, the EU was not party of any of these aforementioned international treaties[66] – including the ECHR. Yet with the fact that all EU Member States are parties of the CoE,[67] the relationship between the ECHR and the EU in matter relating to human rights, consequently, has become more complex. The foundations of the rights protection within the EU legal system are inspired by the integration of human rights norms developed by its Member States and of the norms of the ECHR, including their common national constitutional traditions and international/ European human rights instruments. According to the ECJ's consistent attitude after the *Staunder* case,[68] general principles of EU law including protection for fundamental rights and freedoms are granted.

Additionally, prior to the enactment of the EU Charter of Fundamental Rights,[69] the ECJ treated the ECHR as one of the key sources of the general principles supporting EU law.[70] However, it should be noted that the ECJ held the opinion that the EU in unable to accede to the ECHR because that would exceed the scope of Article 235 of the Treaty without any amendment of it.[71] Nevertheless, it is unlikely for the ECJ to make decisions that run contrary to ECtHR judgements. This is because the supremacy principle of EU law and certain EU Member States' constitutions are

---

[66] The EU itself is not bound by the UN Charter directly but is bound by it indirectly due to the EC Treaty. As regards the ICCPR, it is indeed a source of the general principles of the EU law (for counter opinion, see Case C-249/96 *Grant v. South West Train Ltd.* [1998] ECR I-621, paras. 44-47.) See Craig and Búrca (n 8) 366-369.

[67] Beyleveld, 'Data Protection and Genetics: Medical Research and the Public Good' 281-282.

[68] Case 29/69 *Stauder v. City of Ulm* [1969] ECR 419. This attitude was later confirmed by the *Internationale Handelsgesellschaft* case (Case 11/70 *Internationale Handelsgesellschaft v. Einfuhr- und Vorratstlle für Getreide und Futtermittle* [1970] ECR 1125), the *Second Nold* Case (Case 4/73 *J. Nold v. Commission of the European Communities* [1974] ECR 507) and *Amministrazione delle Finanze delle Stato v Simmenthal* (Case 106/77 *Amministrazione delle Finanze delle Stato v Simmenthal* [1978] ECR 629) See also: Craig and Búrca (n 8) 364-366, Beyleveld, 'An Overview of Directive 95/46/EC in Relation to Medical Research' 6, and Helen Fenwick, *Civil Liberties and Human Rights* (4th edn, Routledge-Cavendish 2007) 138.

[69] Article 6(1) TEU.

[70] Craig and Búrca (n 8) 366-367.

[71] ECJ, Opinion 2/94, 28 March 1996. See also: Fenwick (n 68) 138 and Craig and Búrca (n 8) 367.

bound by ECtHR decisions.[72]

Precisely because of the complex nature which generates potential conflicts, one of the reasons[73] for the EU's accession, according to the CoE, is to reconcile the conflict between two different human rights protection legal frameworks and achieve 'a coherent system of fundamental rights' protection across Europe.'[74] This is addressed in Articles 6(2) and 6(3) of the Treaty of the European Union.[75] On the other hand, the legal basis for the accession of the EU is provided in Article 59(2) of the ECHR, amended in Protocol No. 14 to the ECHR. However, **before the successful/ completely accession** to the ECHR,[76] the ECJ, in the data protection regime,[77] retains the freedom to 'go beyond' the ECHR 'in recognizing rights as part of EU law.'[78] It is observed by Craig and De Búrca that[79]

> It remains to be seen how strictly the ECJ will treat the stipulation that Charter rights corresponding to ECHR rights shall have the 'same' meaning as the ECHR rights,

[72] Deryck Beyleveld, 'Conceptualising Privacy in Relation to Medical Research Values' in Sheila AM McLean (ed), *First Do No Harm: Law, Ethics and Healthcare* (Ashgate Publishing 2006) 158-160.
[73] Craig and Búrca also points out to further reasons, namely to deal with the accusations in relations to the human rights roole of the EU and the sincerety of the attempt to promote the protection of human rights. Craig and Búrca (n 8) 399-400.
[74] The other provided reasons by the Council of Europe include: strengthen the protection of human rights, 'close gaps in legal protection by giving European citizens the same protection vis-à-vis acts of the Union as they presently enjoy vis-à-vis all member States of the Union,' make sure that 'all European legal systems being subject to the same supervision in relation to the protection of human rights,' 'reassure citizens that the EU, just like its member States, is not "above the law" as far as human rights are concerned.' See: Council of Europe, 'Accession by the European Union to the European Convention on Human Rights: Answers to frequently asked questions' (*Council of Europe,* , 2011) <http://www.coe.int/t/dghl/standardsetting/hrpolicy/CDDH-UE/CDDH-UE_documents/EU_accession-QA_2011_en.pdf> accessed 14 May 2012 2-3.
[75] Article 6(2) TEU: 'The Union shall accede to the European Convention for the Protection of Human Rights and Fundamental Freedoms. Such accession shall not affect the Union's competences as defined in the Treaties.' Article 6(3) TEU: 'Fundamental rights, as guaranteed by the European Convention for the Protection of Human Rights and Fundamental Freedoms and as they result from the constitutional traditions common to the Member States, shall constitute general principles of the Union's law.'
[76] The accession by the EU to the ECHR will be successful once the accession agreement has entered into force, which requires the ratification by all member parties to the ECHR as well as the EU itself.
[77] Case C-28/08 *Commission v Bavarian Lager* 29 June 2010.
[78] Craig and Búrca (n 8) 367.
[79] Ibid 367.

but it seems clear that the ECJ is willing to look closely at the relevant ECtHR case law for guidance.

Data protection and the right to privacy are included in the general principles of EU law.[80] In light of this, the interpretation of the Data Protection Directive (and the Data Protection Acts of Member States at national level, which are intended to implement the Data Protection Directive) must take the ECHR into account. This can be confirmed by reading Recital 10[81] and Article 1.1 in conjunction with Recital 1 of the Data Protection Directive. It has been frequently observed that the influence of European human rights law is increasing perceptibly after the Amsterdam Treaty came into force.[82] This has been affirmed by the Treaty of Lisbon. Consequently, the implementation of EU instruments into domestic law is subject to respect for the ECHR.

5.2.1.3.2 The Data Protection Directive and the Data Protection Convention

As the Data Protection Directive builds on the Data Protection Convention (Recital 11), unsurprisingly, the main structures of these two data protection instruments are alike. For example, elements of core data protections principles and other provisions such as mechanisms for mutual assistance and consultation can be found in both of the documents. Several differences, however, can be distinguished. Firstly, as Nouwt

[80] Cases C-465/100, 138 and 139/01 *Rechnungshof v. Österreichisher Rundfunk* [2003] ECR I-12489.
[81] Recital 10 of the Data Protection Directive: 'Whereas the object of the national laws on the processing of personal data is to protect fundamental rights and freedoms, notably the right to privacy, which is recognized both in Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms and in the general principles of Community law…'
[82] Fenwick (n 68) 138.

observes, the Data Protection Directive provides a more detailed content and attracts more attention than the Data Protection Convention, which in turn focuses on administrative obligations.[83]

Secondly, before the Lisbon Treaty, the Data Protection Directive concentrated mainly on the first pillar of the EU, while the Data Protection Convention provides a more common framework, in particular for the police sector (the third pillar).[84] However, it should be emphasised that the EU and the Data Protection Directive 'protect fundamental freedoms and rights only arises for the reason that this protection is deemed necessary for achieving the purposes of the single market.'[85] Nevertheless, it has been suggested that there is a trend indicating that 'the EU is shifting towards the DP regime of the CoE'[86] and a common approach for data protection for both the CoE and the EU.[87]

Thirdly, the respective scopes of personal data within these two documents are defined differently. The Data Protection Convention defines its scope on *automatic* processing of personal data[88] while the Directive extends its scope on applying to the processing of personal data 'wholly or partly by automatic means, and to the processing *otherwise* than by automatic means of personal data which form part of a filing system or are intended to form part of a filing system.'[89] The Directive is subsequent to the Convention and it is much more common to process personal data through an automatic method due to the advanced technologies and the need to

[83] Nouwt (n 49) 289-290.
[84] Ibid 290.
[85] Beyleveld, 'An Overview of Directive 95/46/EC in Relation to Medical Research' 6.
[86] Nouwt (n 49) 286. He reasons this by giving two reasons: first, the EU is now extending the data protection law framework to the third pillar; secondly, the human rights approach is also becoming important to the EU. The latter reason is later confirmed by the content of the Lisbon Treaty.
[87] Ibid 290.
[88] Article 1 of the Convention.
[89] Article 3 of the Directive.

process more complex personal data. The Directive thus demands the protection of individuals that 'must apply as much to automatic processing of data as to manual processing' and 'the scope of this protection must not in effect depend on the techniques used, otherwise this would create a serious risk of circumvention.'[90] Hence, processing personal data by using any kind of technique, either in advanced or simple ways, is not the key point here. However, this does not mean that the scope of the Directive is unlimited. According to Recital 27, 'files or sets of files as well as their cover pages, which are not structured according to specific criteria, shall under no circumstances fall within the scope of this Directive.' This is because in processing such data it is barely possible to interfere with fundamental rights and freedoms of individuals, especially the right to privacy, since one cannot be identified, or at least cost disproportionate efforts to do so.

5.2.1.4 The United Kingdom: Data Protection Law at National Level

The UK has followed the dualist approach[91] which is also accepted in Taiwan. Having ratified the ICCPR and the International Covenant on Economic, Social and Cultural Rights (ICESCR) in 2009,[92] Taiwan is now discussing how to implement the rights protected by these international human rights instruments. There is a chance for Taiwan to learn from other experiences to some degree by understanding the practice of how to deal with the horizontal effect of the Human Rights Act 1998 (HRA) in relation to the jurisprudence of the ECHR. For example, the biometric issue in

[90] Recital 27 of the Directive.
[91] Antonio Cassese, *International Law* (2nd edn, OUP 2005) 214-215.
[92] Act to Implement the International Covenant on Civil and Political Rights and the International Covenant on Economic, Social and Cultural Rights, promulgated on 22 April, 2009. For both Chinese and English edition, see: <http://www.humanrights.moj.gov.tw/lp.asp?ctNode=26507&CtUnit=8379&BaseDSD=7&mp=200> accessed 24 April 2010.

relation to the ID cards policy in the UK, which refers to the question of how to strike a balance explored in this thesis, has been discussed broadly. Consequently, the Taiwanese legislative context and policy could embrace certain features of biotechnology law in respect of data protection and privacy considerations as set out in the UK legislation, in particular the HRA and the Data Protection Act 1998 (DPA). These will be analysed below as an example to understand the Data Protection Law at the domestic level.

5.2.1.4.1 Domestic Influence of EU law

The EC/ EU Treaties are international agreements. Since the UK has followed the dualist approach, international conventions and treaties can enter into effect provided they have been approved by Parliament. Required by UK membership, the implementation of the European Communities Act 1972 fulfilled the need to incorporate existing Community law and to be able to take necessary steps for future Community legislation to take effect.

According to Article 288 TEU, Member States must ensure the compliance of their domestic legislation with the directive before the end of the implementation period expires. The Data Protection Directive requires implementation in Member States by 24th October, 1998. Data protection legislation has been implemented by most EU Member States at various stages (although only Sweden met the deadline).[93] EU legislation often calls for implementing action by the national authorities. However, some important matters are dealt with through an Act of Parliament – in this

[93] The Status of implementation of data protection Directive 95/46/EC could be found at: <http://ec.europa.eu/justice_home/fsj/privacy/law/implementation_en.htm#ukingdom> accessed 24 April 2010.

case, the DPA, which implements the Data Protection Directive.[94]

It is observed by Craig and De Búrca that one of the most problematic issues is the doctrine of direct effect of EC law.[95] For example, due to the weak nature of Article 258 TEU, direct effect could only be applied in public enforcement law.[96] For private enforcement law aspects (which individuals can use to challenge local courts and national action that are against the Community legal order), the ECJ offers direct effects with certain conditions, which were gradually loosened by the ECJ.[97]

This also occurs with regards to the effect of directives. The ECJ held the opinion that directives could have direct effect in principle in the *Van Duyn*[98] and the *Ratti* case.[99] However, the ECJ gives the consistent opinion that directives are capable of direct effect merely in a *vertical* way, meaning that they could be brought before the courts against the States (or state entities), but do not have *horizontal direct effect* which imposes obligations on a private party.

As regards the indirect effects of directives, the ECJ holds that, in many aspects, the Member States have some freedom of action in implementing the directives. However, this is not unlimited.[100] In the *Marleasing* case[101] and in later cases such as *Johnson v MDU*,[102] the ECJ held that the national court's obligation is to interpret

---

[94] Colin Turpin and Adam Tomkins, *British Government and the Constitution* (6th edn, CUP 2007) 321. For a detailed description and analysis of the DPA, see: Peter Carey, *Data Protection: A Practical Guide to UK and EU Law* (3rd edn, OUP 2009).
[95] Craig and Búrca (n 8) 180.
[96] Paul Craig, 'Once upon a Time in the West: Directive Effect and the Federalization of EEC Law' (1992) 12 Oxford Journal of Legal Studies 453. Also, Craig and Búrca, *EU Law: Text, Cases and Materials* (n 8) 181.
[97] Craig and Búrca, *EU Law: Text, Cases and Materials* (n 8) 181, 186-188.
[98] Case 41/74 *Van Duyn v. Home Office* [1974] ECR 1337, para 12.
[99] Case 148/78 *Pubblico Ministero v. Tullio Ratti* [1979] ECR 1629, para 23.
[100] Case C-553/07 *The College van burgemeester en wethouders van Rotterdam v Rijkeboer* [2009], paragraph 56.
[101] Case C-106/89 *Marleasing SA v La Comercial Internacional de Alimentación SA* [1990] ECR I-4135.
[102] *Johnson v Medical Defence Union* [2007] EWCA Civ, para 90.

domestic legislation, so far as possible, in the light of the wording and purposes of a directive and thereby comply with EU obligations. This includes the obligation arising from a directive, which applies even in a horizontal situation. Furthermore, in the *Von Colson* case[103] the ECJ established the principle of consistent interpretation,[104] according to which national courts are under an obligation to interpret national law *at all possible* to avoid a conflict with the Community law.[105] Also, the supremacy of EC law is declared since the *Van Gend en Loos* case[106] and the UK courts has accepted this since the *Factortame* case.[107]

On the other hand, it is well established in the UK that where domestic legislation implements a directive of the European Community, the domestic legislation must so far as possible be interpreted in conformity with the directive. As Sir John Laws posited in *Thoburn v Sunderland City Council*, the UK court is under the duty when delivering a final judgment to override any rule of national law found to be in conflict with any directly enforceable rule of Community law.[108]

Nevertheless, due to the 'negotiated' character of EU legislation,[109] some domestic implementations may not interpret and apply the purposes of the EU law effectively and consistently. This surfaced when applying directives, which are one of

[103] Case 14/83 *Von Colson and Kilmann v Land Nordrhein-Westfalen* [1984] ECR 1891.
[104] Paul Craig and Gráinne De Búrca named this as 'the principle of harmonious interpretation'. See Craig and Búrca, *EU Law: Text, Cases and Materials* (n 8) 200-207.
[105] It is worth noting that in *Marleasing SA v La Comercial Internacional de Alimentación SA*, it goes further to require the national courts to interpret domestic law so as to ensure achievement of the objectives of the Directive. However, Case C-334/92 *Wagner Miret v Fondo de Guarantia Salaria* [1993] ECR I-6911, subsequently, with slightly conservative attitude, holds the opinion which allow national courts to go against pre-existing domestic law, but still requires national courts to interpret national law *at all possible* to avoid a conflict with the Community law. See also, Beyleveld, 'Data Protection and Genetics: Medical Research and the Public Good' 277.
[106] Case 26/62 *Van Gend en Loos v Nederlandse Administratis der Belastingen* [1963] ECR 1.
[107] *R v Secretary of State for Transport ex parte Faetortame (No 2)* [1991]1 AC 603 (HL).
[108] *Thoburn v Sunderland City Council* [2003] QB 151.
[109] Jean-Claude Piris, 'The legal orders of the European Community and of the Member States: peculiarities and influences in drafting' (2005) 58 Amicus Curiae24-25.

the main 'instruments of harmonization'[110] used widely by EU institutions. This can be found in the DPA, for example, that the definition and scope of 'relevant filing system' given in s.1(1)(c) was explained by the House of Lord in a rather narrow way as mentioned above in the *Durant* Case. However, considering the opinions given by the ECJ to interpret provisions of national law so as to comply with the terms of a directive, this decision is open to criticism and in fact controversial.

In the UK, it is the DPA that implements the Data Protection Directive. Considering the *Marleasing* case, the obligation to interpret the DPA to comply with the Data Protection Directive if at all possible is suggested. However, the Directive is not the only source of legislation that the DPA should take into account when interpreting its provisions. Since the Data Protection Directive gives effect to fundamental rights and freedoms protected in the ECHR, the DPA interpretations must therefore take into account the Convention rights. This *interpretive obligation* in the UK, *at the same time*, is declared by s.3 of the HRA. Hence, it is essential to address the domestic influence of the ECHR in the UK, particularly the HRA.

5.2.1.4.2 Domestic Influence of the ECHR: Human Rights Act 1998

The UK was the very first country to ratify the ECHR in 1951, and the Convention came into force in 1953. The jurisdiction of the ECtHR was granted by the UK in 1966, which is much earlier than the introduction of the HRA. The nature of the relationship between the ECHR and the HRA, in particular the Convention rights under the HRA as a species of constitutional rights, is rather complex. It can be divided into two axes.

[110] Craig and Búrca, *EU Law: Text, Cases and Materials* (n 8) 187-188.

The vertical axis refers to the accomplishment of individuals' constitutional rights against the state. Before the entry into force of the HRA, British citizens could only access the ECHR rights and freedoms through the exhaustion of domestic judicial remedies. This is because the ECHR provisions did not have the direct internal legal effect or valid enforcement in the UK[111] before 2nd October, 2000.[112]

Since the HRA entered into force, the domestic impact of the ECHR can be observed in three aspects: legislation, Parliament and case law.[113] This is partly reflected in the s.2(1) of the HRA in relation to the flexible obligation for the courts to 'take into account' the Strasbourg jurisprudence. Although the local courts showed their increasing willingness to 'take into account' the ECHR provisions before the appearance of the HRA,[114] this was not always the case.[115] After the HRA, the House of Lords, more or less, showed the willingness of their lordships to treat the Strasbourg decisions as an expression of fundamental principles.[116] However, the UK courts can still treat the Strasbourg case-law less as binding authority (with the risk of being challenged at the ECtHR and may result in a hefty fine that the UK must pay the applicant.)

Such a 'hesitant' attitude can be explained in various ways. Considering the separation of powers, for instance, the democratic legitimacy question on transferring power from the elected arms of government on human rights grounds to the courts –

---

111 *R v Secretary of State for the Home Department, ex p Brind* [1991] 1 AC 696.

112 This is the date which the HRA came into force in England and Wales, other areas in the UK has already done the procedure before this date. See: Ian Leigh and Roger Masterman, *Making Rights Real: The Human Rights Act in its First Decade* (Hart Publishing 2008) 5-6, citation 16.

113 Turpin and Tomkins (n 94) 273-278.

114 E.g., *Rantzen v Mirror Group Newspapers* [1994] QB 670, 691 and *Derbyshire County Council v Times Newspapers* [1992] QB 770.

115 *Derbyshire County Council v Times Newspapers* [1993] AC 534. For a more detailed description of domestic influence of the ECHR before the HRA, see: Turpin and Tomkins (n 94) 270-271, Leigh and Masterman (n 112) 5-13.

116 *R. v. DPP, ex parte Kebilene* [2002] 2 AC 326, 380-1, *per* Lord Hope of Craighead.

the ECtHR and the domestic courts – will need some further considerations. This consequently draws certain research attention.[117] From the view of constitutional interpretation, both intentionalism and textualism supporters would argue that due to the lack of legal certainty and publicity, the ECHR, which is produced by non-elected arms, is not able to guide individuals' conduct.[118]

Another question raised here is the authority of a 'higher court' in relation to the sovereignty issue. This controversy mainly concentrates on the margin of interpretative autonomy: domestic courts are not bound by the Strasbourg decisions, but merely need to take them into account. The court's autonomy and ability to interpret the law freely is constrained by s.3(1) and s.6 of the HRA. For example, one of the architects of the HRA, Lord Irvine of Lairg, who was also the then Lord Chancellor when the HRA was adopted, suggested that the UK courts should not be bound to follow the ECtHR jurisprudence.[119] On the other hand, in a controversial decision regarding personal data protection, the House of Lords pointed out that it should not extend a protection of the 'Convention Right' through broadening the scope of the right in question unless the Strasbourg Court ever authorised to do so before.[120] Overall, as Masterman describes, 'the HRA leaves open the question of whether it would be legitimate for a domestic court to develop its own reading of the

[117] E.g., Roger Masterman, 'Aspiration or Foundation? Tha Status of the Strasbourg Jurisprudence and the 'Convention Rights' in Domestic Law' in Helen Fenwick, Gavin Phillipson and Roger Masterman (eds), *Judicial Reasoning under the UK Human RIghts Act* (Cambridge University Press 2007) 60-63.

[118] For further discussion on the arguments and critics on the view of intentionalism and textualism on interpreting the ECHR, see: George Letsas, *A Theory of Interpretation of the European Convention on Human Rights* (OUP 2007) 58-79.

[119] HL Debs., 18 November 1997, vol. 583, col. 514.

[120] *R. v. Chief Constable of South Yorkshire* [2004] UKHL 39, Lord Steyn, para 27; Lord Rodger, para 66; Lady Hale para 78. The same case was later in the ECtHR: *S and Marper v UK* (App nos 30562/04 and 30566/04) ECHR 4 (App nos 30562/04 and 30566/04) ECHR 4. See also: *Regina v. Special Adjudicator ex parte Ullah; Doe v. Secretary of State for the Home Department* [2004] UKHL 26, Lord Bingham of Cornhill described at paragraph 20 that '…the ECHR is an international instrument, the correct interpretation of which can be authoritatively expounded only by the Strasbourg court…'

compatibility of a provision with the Convention right.'[121]

Criticisms have been made in light of Strasbourg case-law. First, the appellants may, due to the need to appeal their case to the Strasbourg Court in order to accomplish certain Convention rights, bear the burden of delay and cost and suffer from long court activities.[122] Secondly, it is arguable that the aforementioned attitude does not fit in with the spirit of 'bringing rights home' which is aimed by the HRA. To hold an opinion which is not compliant with the main purpose of the law discussed here is, therefore, unwise.

As regards to the 'horizontal rights,'[123] under traditional international law, individuals can have merely vertical rights as addressed above. In other words, private parties cannot raise legal proceedings against another private individual which is not 'the High Contracting Parties' (i.e. the State).[124] This is also applied in the ECHR machinery, though there is an exception of the right to petition under Article 35. The major controversy in the UK regarding whether Convention rights have horizontal effect, as Ian Leigh and Roger Masterman observe, is about the protection of the right to privacy.[125] This is because the text of Article 8 of the ECHR refers to only public authorities and does not give a clear indication about whether the right to privacy in the ECHR is capable of both vertical and horizontal effect.

In terms of this argument, some English judgements do not fully adopt the

---

[121] Masterman (n 117) 63.
[122] See also, ibid 76-86, Ian Leigh, 'Concluding Remarks' in Helen Fenwick, Gavin Phillipson and Roger Masterman (eds), *Judicial Reasoning under the UK Human RIghts Act* (CUP 2007) 435-440.
[123] It refers to the application of human rights when the infringer is an individual or a private legal person.
[124] Article 34 of the ECHR: 'The Court may receive applications from any person, non-governmental organisation or group of individuals claiming to be the victim of a violation by one of the High Contracting Parties of the rights set forth in the Convention or the Protocols thereto…'
[125] Leigh and Masterman, *Making Rights Real: The Human Rights Act in its First Decade* (n 112) 239.

concept of the direct horizontal effect.[126] However, this has been surpassed by the *Von Hannover* case[127] which points out that Article 8 requires Member States to assume a positive duty to offer domestic remedy for violations of the right to private life by private individuals. Moreover, since the DPA reaches fully between the private parties in the UK, it is suggested that *at least part* of the rights protected by Article 8 of the ECHR may bind private bodies in the UK.[128] The key question of this issue, as addressed by scholars, is 'whether further adjustments will be required to give full effect to *Von Hannover* case since it is clear that English courts must now look in determining what counts as private information.'[129]

5.2.2 Data Protection Law Regarding Applications of Biometric and RFID

The so called 'new technologies' share a common characteristic: they always develop much faster than regulation. It has been remarked by Brownsword that, as indicated by our experience, these attractive technologies tend to 'create difficulties to regulators.'[130] As biometric and RFID technologies are rapid-developing technologies, it is unsurprising that there are relatively few regulations focusing specifically on these new technologies in Europe. It is noted that most of the biometric and RFID legal frameworks concentrate on data protection perspective due to their implication

---

[126] *Wainwright v Home Office* [2004] 2 AC 406, [2003] UKHL 53. Also, *Campbell v. MGN* [2004] UKHL 22. See: Leigh and Masterman, *Making Rights Real: The Human Rights Act in its First Decade* (n 112) 248-252. Also, Gavin Phillipson, 'Clarity Postponed: Horizontal Effect after Campbell' in Helen Fenwick, Gavin Phillipson and Roger Masterman (eds), *Judicial Reasoning under the UK Human RIghts Act* (Canbridge University Press 2007) 143-173.

[127] *Von Hannover v. Germany* (2005) EHRR 41.

[128] Cf. Fenwick (n 68) 936.

[129] Leigh and Masterman, *Making Rights Real: The Human Rights Act in its First Decade* (n 112) 252.

[130] Roger Brownsword, 'So What Does the World Need Now? Reflections on Regulating Technologies' in Roger Brownsword and Karen Yeung (eds), *Regulating Technologies: Legal Futures, Regulatory Frames and Technological Fixes* (Hart Publishing 2008) 26. Also, Roger Brownsword, *Rights, Regulation, and the Technological Revolution* (OUP 2008) 160-184.

on collecting and processing of personal data.

At EU level, the European Council issued Regulation EC 444/2009 which amends Regulation EC 2252/2004 on standards for security features and biometrics in passports and travel documents issued by Member States. Two specific groups are excluded from providing fingerprints: (1) children under the age of 12, (2) persons physically unable to provide fingerprints.[131] This exemption responds to the concerns we mentioned in section 2.2.3.

The WP29 also continually pays attention to this. WP 80 regarding the application of data protection principles of the Data Protection Directive,[132] for example, particularly focuses on the principle of purpose specification and principle of proportionality.[133] Further opinions such as WP 96,[134] WP 112,[135] and WP 134[136] on the biometric passport and travel documents have since been adopted.

With regard to the CoE, on the other hand, according to the progress report on the application of the principles of Convention 108 to the collection and processing of biometric data,[137] the T-PD concludes that the fundamental data protection principles

---

[131] Article 1(1).
[132] Working document on biometrics, adopted on 1 August, 2003, < http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2003/wp80_en.pdf> accessed 24 April 2010.
[133] Ibid., section 3.2 at 6-8.
[134] Opinion No 7/2004 on the inclusion of biometric elements in residence permits and visas taking account of the establishment of the European information system on visas (VIS), adopted on 11 August 2004, < http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2004/wp96_en.pdf> accessed 24 April 2010.
[135] Proposal for a Council Regulation on standards for security features and biometrics in EU citizens' passports, adopted on 30 September 2005, < http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/others/2004-11-30-eupassports_en.pdf> accessed 24 April 2010.
[136] Opinion N° 3/2007 on the Proposal for a Regulation of the European Parliament and of the Council amending the Common Consular Instructions on visas for diplomatic missions and consular posts in relation to the introduction of biometrics, including provisions on the organisation of the reception and processing of visa applications (COM(2006)269 final), adopted on 1 March 2007, < http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp134_en.pdf> accessed 24 April 2010.
[137] The Consultative Committee of the Convention for the Protection of Individuals with regard to

are relevant to biometric technology in its recent report and reflects these principles to this developing technology.[138] These principles include, for instance, the principle of purpose,[139] the principle of proportionality,[140] and the principle of precaution.[141] It also points out the close relation between human rights, human dignity, and biometrics at both international and national level.[142] It further recommends to take '*precautions* to avoid possibly irreversible developments that are not aimed at but contain considerable and unnecessary drawbacks for the protection of personal data'[143] (*emphasis added*). It has been observed, however, that while this report emphasises on the importance of the data protection principles, it remains silent on the question as to whether there is a *real* free choice for individuals could be taken part in daily life with respect to biometric applications[144] – both in the public and private

---

Automatic Processing of Personal Data, 'Progress Report on the Application of the Principles of Convention 108 to the Collection and Processing of Biometric Data' (*T-PD*, 2005) <http://www.coe.int/t/e/legal_affairs/legal_co-operation/data_protection/documents/reports_and_studies_of_data_protection_committees/2Biometrics_2005_en.pdf> accessed 13 February 2010. There are several recommendations and surrounding reports could be considered as being relevant to biometric technology and data protection. For example: Recommendation No.R(87) 15 regulating the use of personal data in the police sector (17 September 1987) and its three Evaluation Reports, Recommendation No.R(89) 2 on the protection of personal data used for employment purposes (18 January 1989) and Explanatory Memorandum, Recommendation No.R(91) 10 on the communication to third parties of personal data held by public bodies (9 September 1991) and Explanatory Memorandum, Recommendation No.R(97) 5 on the protection of medical data (13 February 1997) and Explanatory Memorandum, Report containing guiding principles for the protection of individuals with regard to the collection and processing of data by means of video surveillance (2003), Guiding principles for the protection of personal data with regard to smart cards (2004), and Study on the introduction and use of personal identification numbers: the data protection issues (1991).
However, these materials are merely of some relevant to biometrics issues. The only official document approved by the CoE that concentrates on biometrics usage, indeed, is the progress report itself.

[138] Ibid, paras 106-107.

[139] This report expressed the attitude of following the principle of purpose when deciding the criteria to choose the system architecture. See: ibid, paragraph 43.

[140] It is stressed by the T-PD that any exceptional circumstances of the principle of purpose in deciding the criteria to choose the system architecture should consider particularly the requirement of the principle of proportionality in accordance with Article 8 paragraph 2 of the ECHR. See: ibid, paragraph 49.

[141] It is addressed in this report when considering the sensitive nature of biometric data, it must bear in mind that '[t]he precautionary principle demands that where new techniques may uncover unexpected new information one should be reticent to start with systems where there can be reasonable doubt that in the long run unwanted and possibly irreversible side effects may appear.' Ibid, paragraph 74.

[142] Ibid, paras 106-107.

[143] Ibid, paragraph 15.

[144] Yue Liu, 'Identifying Legal Concerns in the Biometric Context' (2008) 3: 1 Journal of International Commercial Law and Technology49-50. Also, The Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, paragraph 58.

sectors.

As regards RFID, the Commission of the European Communities issued the recommendation on the implementation of data protection principles in supplications supported by the RFID in 2009 (2009 Recommendation).[145] This document aims to provide the requested clarification and guidance on the data protection and privacy aspects of RFID applications through one or more Commission Recommendations. [146] In addition to defining certain key terms of RFID, it assesses the impact of the uses of RFID regarding privacy and data protection, in particular the Data Protection Directive. It stresses the importance of information and transparency on RFID applications. Moreover, the WP 29 adopted relevant documents such as WP 105[147] and WP 111.[148]

The 2009 Recommendation furthermore asks States to request the relevant RFID industry and its shareholders to develop a framework to assess the impact of privacy and data protection. This framework has been submitted to the WP29 for endorsement. The WP29 was not satisfied by the first submission and released its opinion, holding that three action points should be fulfilled in the revised version.[149] These three

---

[145] Commission Recommendation of 12.5.2009 on the implementation of privacy and data protection principles in applications supported by radio-frequency identification, < http://ec.europa.eu/information_society/policy/rfid/documents/recommendationonrfid2009.pdf> accessed 24 April 2010.

[146] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions - Radio Frequency Identification (RFID) in Europe: steps towards a policy framework {SEC(2007) 312}, < http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0096:FIN:EN:PDF> accessed 24 April 2010.

[147] Working document on data protection issues related to RFID technology, adopted on 19 January 2005, < http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp105_en.pdf> accessed 24 April 2010.

[148] Results of the Public Consultation on Article 29 Working Document 105 on Data Protection Issues Related to RFID Technology, adopted on 28 September 2005, < http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp111_en.pdf> accessed 24 April 2010.

[149] Opinion 5/2010 on the Industry Proposal for a Privacy and Data Protection Impact Assessment Framework for RFID Applications, WP 175, 13 July, 2010, < http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp175_en.pdf >, accessed 26 July, 2011.

requirements include: (1) to produce a well-defined risk assessment approach for privacy and data protection impact (PIA);[150] (2) to consider RFID tags carried by persons without noticing or valid consent; and (3) to consider the tag deactivation principles in the retail sector. What is worth noting here is that the opinion, with respect to the second requirement, contends that when a RFID tag is associated to an *identifiable* data subject, no matter whether she is identified or not, the definition set forth in the Data Protection Directive is called into play. This is crucial since the nature of the RFID applications raises the possibility of a data subject to be tracked by RFID application operators without her being aware of it. This is in agreement with what was discussed in section 5.2.1.2.2 with respect to Recital 26 of the Directive. A subsequently revised framework has been submitted to the WP29 in this regard. It has been endorsed in Opinion 9/2011.[151]

5.3 The Right to Privacy in Taiwan: the Status Quo

A different legal system which profoundly transplants Western jurisprudence and applies European data protection principles makes its regulatory position worth researching. During this process, I will begin this inquiry by surveying Formosan primary statutory privacy and data protection provisions and surrounding constitutional interpretations, followed by a section critically examining the contents of the right to privacy. The issues that need to be analysed further through the lens of the PGC will also be identified.

[150] For a detailed discussion, see section 7.2.2.

[151] Opinion 9/2011 on the revised Industry Proposal for a Privacy and Data Protection Impact Assessment Framework for RFID Applications, WP 180, 11 February, 2011, < http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp180_en.pdf >, accessed 26 July, 2011.

5.3.1 The Statement of the Right to Privacy

Traditionally, under the profound cultural influences of the Chinese immigrants and the Nationalists Party (KMT) which fled in 1949, there was no legal foundation regarding the right to privacy in Taiwan.[152] Unsurprisingly, therefore, the relatively 'modern/ young' concept of the right to privacy is not one of the constitutionally enumerated fundamental rights in Taiwan.[153] Some inter-related reasons can be offered. Firstly, the demand to take the right to privacy as a constitutional right was weak. As it is universally observed, the first right to privacy article was published by Samuel D. Warren and Louis D. Brandeis in their famous contribution *The Right to Privacy* in 1890. However, to consider it as a type of fundamental right and freedoms is a rather long process. For example, in the international law domain, the right to privacy was later stated in the Universal Declaration of Human Rights (UDHR) in 1948 and enshrined in the ECHR in 1950. It is thus difficult for Taiwan's legal system to transplant and borrow Western jurisprudence and legal experience to include the right to privacy that developed so late.

Secondly, in Taiwan, the change of the Constitution evolves more slowly than expected because of the complex post-Second World War history and the relationship between Taiwan and its mainland neighbour – China (People's Republic of China,

[152] In fact, the right to privacy is discouraged by some Eastern-Asia ancient wisdoms. Confucius, for example, addresses that 'the Gentleman is free and has nothing to hide.' Some commentators argue that the family-oriented system may, at some degree, have the idea of 'private space' from the public perspective. See: Shin-Yi Peng, 'Privacy and the Construction of Legal Meaning in Taiwan' (2003) 37 The International Lawyer 1038-1040. However, the reason why the ancient houses were built in such styles can also be argued as for the defending purpose and the demand of politeness.

[153] Taiwan's (the Republic of China, ROC) Constitution was adopted on 25th December, 1946, by the National Assembly convened in Nanking (China).

PRC). Because of the impasse between the cross-strait governments[154] and the international society (mainly, the USA)[155] in relation to the legal and political status of Taiwan, amending the Constitution is never an easy job. Seven revisions have been made mainly due to the need to meet the demands of constitutional rule before the 'national unification' of 'the Republic of China.'[156] Consequently, it is unsurprising that most constitutional changes have focused on the governmental institutions such as the Legislative Yuan (the parliament), the National Assembly, the elections of the Honourable Justices of the Judicial Yuan (the court), and the president, rather than deploying the values of fundamental rights and freedoms. Consequently, the attempts of listing any new type of fundamental rights in Taiwan's constitution are much more complex than other 'ordinary nations.'[157]

However, this does not mean that there is no demand of judicial effort with regards to emerging rights or interests. Actually, such a demand is undoubtedly enormous, particularly when facing profound transformations, starting from a

---

[154] Banyan, 'Taiwan's Commonsense Consensus: Economic Integration with China Is not Doing What China Hoped and the Opposition Feared' *The Economist* (London, 24 February 2011) <http://www.economist.com/node/18229208> accessed 5th March, 2011.

[155] For example, in a report written by the National Committee on American Foreign Policy, the project director addresses that '… we need to make clear to Taiwan that although America supports Taiwan's democracy and will stand by its obligations under the Taiwan Relation Act, those obligations do not involve handing Taiwan a blank check. Taiwan's leaders must consult with us on any actions or policies that could threaten cross-strait stability, including the revision of the Taiwan Constitution. *The process of changing the Taiwan Constitution must be a transparent one, and the views and the cautionary notes bring expressed by the United States need to be taken into account*…' (emphasis added). See: Donald S. Zagoria, *The Taiwan Challenge* (the National Committee on American Foreign Policy presneted to the Asia Society, 2004) 6. Also, Banyan, 'America's Security Commitment to Taiwan: From Keystone to Millstone?' *The Economist* (London, 3 March 2011) <http://www.economist.com/blogs/banyan/2011/03/america%E2%80%99s_security_commitment_taiwan> accessed 5 March 2011.

[156] For the official English translation of Taiwan's Constitution and the reversions, see: <http://english.president.gov.tw/Default.aspx?tabid=434> accessed 3 March 2011.

[157] The seventh revision of the constitution states that 'Amendment of the Constitution shall be initiated upon the proposal of one-fourth of the total members of the Legislative Yuan, passed by at least three-fourths of the members present at a meeting attended by at least three-fourths of the total members of the Legislative Yuan, and sanctioned by electors in the free area of the Republic of China at a referendum held upon expiration of a six-month period of public announcement of the proposal, wherein the number of valid votes in favour exceeds one-half of the total number of electors, ' which leads a relatively high threshold to amend the constitution.

totalitarian regime and moving towards a new constitutional democracy[158] and the extending gap between the rapid technology developments and the delay in legal change.[159] To meet the aforementioned demands, the constitutional interpretations (issued by the Honourable Justices of the Judicial Yuan, hereinafter 'J. Y. Interpretation') help to 'push forward the changing of the Constitution over time.'[160] The right to privacy, for example, has attracted both scholarly research and civil-society/ civil rights movements for more than one decade in Taiwan.

Overall, the Formosan modern legal framework regarding the right to privacy is noticeably ambiguous by virtue of the lack of historical foundation of the idea of privacy. The constitutional privacy framework is therefore left to constitutional interpretations. An overview of Taiwan's constitutional privacy framework and personal data protection framework is needed in order to help understand the circumstance of this demand and the current responses – and of course, some of the challenges it poses.

5.3.2 The Constitution and Its Privacy Framework

Although the right to privacy is not a clearly listed fundamental human right under Taiwan's Constitution, the term 'privacy' can be found in the main text of the Constitution. It is stated in Article 12:

---

[158] Cheryl Saunders and others, 'Asian Constitutions in Comparative Perspectives' (2009) 4 National Taiwan University Law Review 204.

[159] The second revision of the constitution has acknowledged the challenge and therefore states that 'the focus of fundamental national policies is expanded to include promotion of culture, science and technology, environmental protection, and economic development, and to safeguard the interests of women, aborigines, the handicapped, and the people of offshore islands.'

[160] Wen-Chen Chang, 'The Role of Judicial Review in Consolidating Democracy: the Case of Taiwan' (2005) 2 Asia Law Review 73.

[t]he people shall have freedom of privacy of correspondence.

However, this article actually regards the freedom of correspondence rather than the right to privacy. Arguably, privacy of correspondence can be considered under the concept of the right to privacy.[161] Similarly, it is also arguable that the rights protected under Articles 13[162] and 14,[163] namely, freedom of religious belief and freedom of assembly and association may include certain concepts of privacy.[164] However, even from a view of intentionalism, it remains unlikely that this reflects the intentions of the constitutional drafters. Moreover, the above arguments are unable, at least barely so, to explain the whole concept of the right to privacy itself.[165] It is, therefore, unlikely to make a reliable statement saying that Article 12 introduces a *general* idea of the right to privacy.

The term 'privacy' can also be found in the words of the Honourable Justices. It is quite interesting to see how the Formosan Constitutional Court repeatedly refers to the fundamental rights and freedoms, the right of personality, and the self-development principles to justify the recognition of this 'modern right'. The first privacy concern can be read from J. Y. Interpretation No. 293 in 1992.[166] However, whether the status of privacy was a right under the protection of the Constitution remained unclear.[167] It was until J. Y. Interpretation No. 535 in 2001 the

[161] In J. Y. Interpretation No. 631 the Honourable Justices point out that 'The freedom of privacy of correspondence is one of concrete modes of right to privacy that the Constitution guarantees.'
[162] Article 13: The people shall have freedom of religious belief.
[163] Article 14: The people shall have freedom of assembly and association.
[164] Privacy International, 'PHR2006 - Republic of China (Taiwan) ' (*Privacy International*, , 2007) <https://www.privacyinternational.org/category/countries/taiwan> accessed 5 March 2012.
[165] Comparing with Article 8 of the ECHR which consists protection of private and family life, home and *correspondence*, Article 12 of Taiwan's Constitution only refers the correspondence interest.
[166] It is noted that in J. Y. Interpretation No. 293, three Honourable Justices consider the right to privacy should be interpreted as a constitutional right.
[167] Tzu-Yi Lin, 'Genetic Information and Genetic Privacy: the Processing and Legislative Framework of Genetic Information from the Perspective of Protecting the Right to Privacy' in The Editing Committee on Celebrating the Seventieth Birthday of Professor Yueh-Sheng Weng (ed), *Contemporary Public Law Issues*, vol 2 (Angel Publisher 2002) 700. Also, Fu-Te Liao and Yi-Hung Weng, 'Dilemma

Constitutional Court regards the right to privacy as a type of fundamental rights and freedoms:

> … However, the ways in which police checks are conducted including searches, street checks, and interrogations may have a great effect upon personal freedom, right to travel, property right and *right to privacy* and therefore such checks must be in accordance with the rule of law as well as legal principles guiding police functions and legal enforcement. Thus, to fully ensure the *constitutional* protection of people's *fundamental rights and freedoms*, the requirements and procedures of police checks as well as legal remedies for unlawful checks must be prescribed clearly in the law… (emphasis added)

This opinion was then reaffirmed by J. Y. Interpretation No. 585 in 2004:

> *The right of privacy, though not clearly enumerated under the Constitution, is an indispensable fundamental right protected under Article 22 of the Constitution* because it is necessary to preserve human dignity, individuality, and the wholeness of personality development, as well as to safeguard the freedom of private living space from interference and the freedom of self-control of personal information (See J.Y. Interpretations Nos. 509 and 535). (emphasis added)

Under this interpretation, an abstract article[168] for safeguarding all the other unlisted types of fundamental rights and freedoms is applied. This interpretative method is

---

or Co-existence: Collecting Individual Information and Protection of Information Privacy' in The Editing Committee on Celebrating the Seventieth Birthday of Professor Chung-Mo Cheng (ed), *Issues on Public Law in the 21st Century* (New Sharing Publishing 2008) 309.

[168] Article 22 states that '[a]ll other freedoms and rights of the people that are not detrimental to social order or public welfare shall be guaranteed under the Constitution.' Article 23 further declares that '[a]ll the freedoms and rights enumerated in the preceding Article shall not be restricted by law except by such as may be necessary to prevent infringement upon the freedoms of other persons, to avert an imminent crisis, to maintain social order or to advance public welfare.'

then followed by J. Y. Interpretation Nos. 603 and 613.[169] As the majority of[170] the Formosan Honourable Justices obtained their law degrees from Germany, it is unsurprising to find out that this approach, which refers to human dignity and the right to personality in order to justify the right to privacy, borrows from the German Constitutional Court's opinions.[171]

5.3.3 General Provisions on the Right to Privacy and Personal Data Protection

5.3.3.1 Legal Framework of the Right to Privacy

As previously noted, the right to privacy does not find its 'Eastern tradition' in Taiwan. Formosan modern privacy framework transplants and migrates from Western jurisprudence. For example, constitutional interpretations repeatedly contend that the core value of the right to privacy, which can be viewed as a value borrowed from the German jurisprudence, is to protect *human dignity*.[172] This is reflected in several contexts of Taiwan's legal fields.

The Civil Code

[169] For the German Constitutional Courts' opinions in relation to the justification of the right to privacy, see: Yves Poullet, 'About the E-Privacy Directive: Towards a Third Generation of Data Protection Legislation?' in Serge Gutwirth, Yves Poullet and Paul De Hert (eds), *Data Protection in a Profiled World* (Springer 2010) 4-5.

[170] Until September 2011, 9 out of 15, and after October 2011, 6 out of 15 obtained their law degrees from Germany.

[171] In an empirical study analysing the patterns of foreign law citations by the Formosan Constitutional Court, it has been observed that 'justices with learning experiences in Germany are more likely to cite German constitutional laws whereas those with learning experiences in the United Stated more frequently cote American constitutional laws.' Wen-Chen Chang, 'Transnational Constitutional Dialogues: An Empirical Study on Foreign Law Citations by the Constitutional Court of Taiwan' in Shu-Perng Hwang (ed), *Constitutional Interpretation: Theory and Practice Vol 7 Part Il* (Institutum Iurisprudentiae, Academia Sinica 2010) 483-518.

[172] J. Y. Interpretation No. 603.

The concept of the right to 'personality', which is cherished by the Constitution, is reflected in Article 18 of the Civil Code. It is considered that, under the Civil Code, the right to privacy is merely indirectly protected in a very vague sense by applying Article 18.[173] It is noted that tort damages could only be recovered by satisfying the burden of proof of damages specifically provided by law (e.g., Article 19 of the Civil Code with respect to the right of the usage of one's name).[174]

It was not until 1999 the term 'privacy' clearly appeared in Taiwan's Civil Code Amendment. In Article 195(I) of the amendment, the value of human dignity and personal integrity was expressly connected to the protection of privacy as an individual interest:

> If a person has wrongfully damaged to the body, health, reputation, liberty, credit, *privacy* or chastity of another, or to another's *personality* in a severe way, the injured person may claim a reasonable compensation in money even if such injury is not a purely pecuniary loss. If it was reputation that has been damaged, the injured person may also claim the taking of proper measures for the rehabilitation of his reputation. (emphasis added)

This article implies that the interference of an agent's privacy could be considered as a type of severe damage of his/ her personality. Therefore, it can be argued that the drafters may refer to the privacy value as a crucial concept of 'personality', which is a reflection of human dignity.

---

[173] Article 18 of the Civil Code states that '(I) When one's personality is infringed, one may apply to the court for removing. When one's personality is in danger of being infringed, one may apply for prevention. (II) In the preceding paragraph, an action for damages for emotional distress may be brought only it is otherwise provided by the act.' For the indirect application to deal with the invasion of privacy prior to the 1999 amendment, see: Peng (n 152) 1046-1047.

[174] Article 19: 'If one's right to use his name is infringed, one may apply to the court for removing of infringement and for damages for emotional distress.'

The Criminal Code

The Formosan Criminal Code concentrates on the breach of confidence in Chapter 28.[175] It begins with Article 315, which states that a person, who, without a reasonable cause, opens or conceals a *sealed* letter or other *sealed* document or picture belonging to another, may be punished under the law. However, the purpose of this article is simply to correspond to Article 12 of the Constitution rather than a direct protection of the right to privacy.

To deal with the need to reduce the gap between the normative framework and technology, the Criminal Code affirmed Articles 315-1 and 315-2 in its 1999 amendment. Article 315-1 states that an individual shall be punished if he uses devices or equipment to peek at, wiretap or eavesdrop, or if he records, photos videotapes or uses any electrical devices to record on other's *private* activities, conversations, or speeches *without any reasonable causes*. If one violates the above rules in pursuit of his own interests or to disseminate, broadcast or sell the content of the above records, Article 315-2 is involved. It should also be noted that the purpose of these articles is to protect the interests of both social welfare and *individual privacy*.

Two points require further discussion. First, the requirements of Article 315 which protect the confidentiality are very similar to the *earlier* (which is the conventionally understood one) English common law idea of the duty of

[175] Some commentators translate the title (妨害秘密罪) of this Chapter as 'Offences against Privacy.' See for example: Peng (n 152) 1045. However, this might not be right. First, throughout this chapter, there is no such an idea of 'privacy.' It must be noted that, until now, the term 'privacy' has not been addressed within the text of the Criminal Code. It was not until the appearance of Articles 315-1 and 315-2, the concepts of the right to privacy was clearly mentioned in the *purpose* of the amendment. Secondly, at the time drafting the Criminal Code, there is no such an idea of 'privacy' in Taiwan. Thirdly, as the author argues below, the aim of Article 315 in the Criminal Code is to protect the interest of confidentiality or the privacy of correspondent under the demand of Article 12 of the Constitution, which is merely one concept of privacy, rather than the right to privacy.

confidentiality. There are three key elements in the English traditional formulation for the action of breaching of confidence:[176]

1. 'The information itself… must have necessary quality of confidence about it;'
2. 'Information must have been imparted in circumstances importing an obligation of confidence;' and
3. 'There must be an unauthorised use of that information to the detriment of the party communicating it.'

Under this formulation, the common law duty on breach of confidence 'was of limited value in protecting privacy, since it only covered those specific instances in which information was communicated in confidence.'[177] This is similar to Article 315 of Taiwan's Criminal Code, which states that one of the elements of violating this legal duty is to open or conceal 'a *sealed* letter or other *sealed* document or picture.'

Secondly, can the subsequent 1999 amendment widen the scope of the duty of confidence protected by Article 315? The answer should be affirmative. This is because the concept of protected interests under Articles 315-1 and 315-2 includes uncovering private facts and activities. Hence, it can be argued that, at least under the Criminal Code, the protection of the right to privacy may now be encompassed (at least to some extent) by the law of confidence. This is also similar to the modern common law trend.[178] Moreover, the new amendment does not mention any exemption in relation to other (constitutional) fundamental rights and freedoms such as the freedom of press. This is again similar to the reshaping of the action for breach

[176] *Coco v. A. N. Clark (Engineers) Limited* [1969] R P C 41, 47. This judgement was then confirmed by *A-G v. Guardian Newspapers (No. 2)* [1990] 1 A C 109.
[177] Helen Fenwick and Gavin Phillipson, 'Confidence and Privacy: A Re-examination' (1996) 55 Cambridge Law Journal 453.
[178] *Hellewell v. Chief Constable of Derbyshire* [1995] 1 W L R 804, 807. Fenwick and Phillipson, 'Confidence and Privacy: A Re-examination' (n 177) 453-454.

of confidence in *Campbell v Mirror Group Newspapers* in English common law, which protects the right to privacy as well.[179]

Nevertheless, this new doctrine is not in every case final and definitive, as stated in Article 23 of the Constitution. Therefore, similar to the argument raised by Fenwick and Phillipson on the English common law regarding confidence and privacy,[180] the 1999 amendment cannot always offer a remedy in certain situations, e.g., the conflict between the freedom of press and the right to privacy.

The Administrative Provisions

There are a number of administrative regulations governing communication and correspondence in response to Article 12 of the Constitution. Such provisions, for example, can be found in Articles 23[181] and 24[182] of the 1996 Radio and Television Act, Articles 61[183] and 62[184] of the Cable Radio and Television Law, and Articles 30[185] and 31[186] of the Satellite Broadcasting Law. However, privacy is not a directly

[179] Deryck Beyleveld and Shaun D. Pattinson, 'Confidentiality and Data Protection' in Andrew Grubb, Judith Laing and Jean McHale (eds), *Principles of Medical Law* (3rd edn, OUP 2010) 655-656.
[180] Fenwick and Phillipson, 'Confidence and Privacy: A Re-examination' (n 177) 454-455.
[181] Article 23 states: 'If an involved party considers a station's report to be erroneous, the said party may request a correction within 15 days of its broadcast. The station shall make the correction in the same program or in another program in the same time slot within seven days of receiving the request. If the station considers that there is no error in the report, it shall make a written response to the said party.
If the erroneous report of the preceding paragraph causes actual impairment to the rights and interests of the involved party, the station, its responsible person, and related personnel shall be liable to civil or criminal charges.'
[182] Article 24 states: 'If radio/television commentaries involve other people or agencies or organizations to the extent of impairing their rights and interests, the stations concerned shall not reject requests by the involved parties for an equal opportunity for defence.'
[183] Article 61 states: 'If an involved party considers a cable radio or television program or advertisement to be erroneous, the said party may request a correction within 15 days of its transmission. The system operator shall make the correction in the same program or advertisement in the same time slot within 15 days of receiving the request. If the system operator considers that there has been no error in the program or advertisement, it shall state its reasons in a written response to the said party.'
[184] Article 62 states: 'When a commentary in a cable radio or television program involves other individuals, institutions, or organizations to the extent that the rights and interests of the involved party are impaired, the request by the said party for a commensurate opportunity to respond shall not be rejected.'
[185] Article 30 states: 'If an involved party considers a satellite broadcasting program or advertisement

protected form of right under these laws: none of these even mention the right to privacy. To look at the right to privacy in the communication aspect, one has to turn to Article 6 of the Telecommunications Act.[187]

The competing interests under Article 6 of the Telecommunications Act have frequently been regarded as public interests defined by the *governmental authorisation*. So, how to reconcile the possible conflicts under this article? The Communications Protection and Surveillance Law may offer us a hint by further regulating that '[n]o interception of communication may be executed, except as necessary to ensure national security or the maintenance of social order.'[188] The aim of this law, contained in Article 1,[189] is *supposed* to prevent illegal spying or surveillance. However, it is rightly observed by Peng that this regulation may have a practical problem: the government, and particularly the police, tends to 'expend its power' to tap into other unregulated new-developing communicating methods.[190] How to deal with this problem?

Although there is no clear criterion to deal with competing rights and interests within the administrative regulatory tools regarding the communication in Taiwan, the

---

to be erroneous, the said party may request a correction within 20 days of its broadcast. The satellite broadcasting business shall make the correction in the same program or advertisement in the same time slot, within 20 days of receiving the request. If the satellite broadcasting business considers that there has been no error in the program or advertisement, it shall state its reasons in a written response to the said party.'

[186] Article 31 states: 'When a commentary in a satellite broadcasting program involves individuals, institutions, or organizations to the extent that the rights and interests of the involved party are impaired, the request by the said party for a commensurate opportunity to respond shall not be rejected.'

[187] It states that 'Communications processed through telecommunications enterprises or dedicated telecommunications shall not be accessed or taped without authorization, nor shall the privacy thereof be violated through other illegal means,' and ' a telecommunications enterprise shall implement appropriate and necessary measures to safeguard the confidentiality of its processed communications.' Article 56.1 further provides that 'Violators of Paragraph 1 of Article 6 regarding infringement on others' secrecy of communications shall be penalized with imprisonment of not more than five years, with a possible fine of not more than NT$1,500,000…'

[188] Article 2 of the Communications Protection and Surveillance Law.

[189] Article 1 states: 'The purpose of this Act is the protection of the people's right of private communication from illegal infringement, ensuring national security and maintaining social order.'

[190] Peng (n 152).

constitutional demand of protecting human dignity should always be taken as the central value. In this regard, it is crucial to bear in mind that, as Article 5 of the Fundamental Communications Act states, that '[c]ommunications shall safeguard *human dignity*, respect minorities' rights and interests, and promote the balanced development of cultural diversity' (emphasis added).

There are other specific administrative rules regulating the media and press in order to protect the right to privacy.[191] However, to understand the general Formosan legal framework of personal data protection, in particular the right to privacy, it is necessary to focus on the Personal Data Protection Law.

5.3.3.2 Personal Data Protection Law

The Computer-Processed Personal Data Protection Law (CPDPL) was promulgated in 1995. Although it seemed to follow a number of data protection principles applied by the primary international/ European legal frameworks, e.g., the OECD Guidelines, the Data Protection Convention and the Data Protection Directive,[192] it has been argued that the 1995 version was unable to protect the rights and interests in relation to

[191] For example, paragraph 4, Article 36 of the Public Television Act states: 'Program production and broadcasting shall respect personal reputations and protect the right of privacy, ' paragraph 1, Article 46 of the Children and Youth Welfare Act states: 'No publicity materials, publications, broadcasting and television, website information or other media shall report or write the name or any information that may be identify the children or youth concerned suffering the behaviours as stated in article 30 or paragraph 1 of article 36…' and paragraph 1, Article 13 of the Sexual Assault Crime Prevention Act states: 'Advertisements, publications, broadcasts, television, electronic messages, computer, internet or other kinds of media should report or record neither the victim's name nor other information which can lead discovery of his or her identity...'

[192] According to the regulations governing the personal data held by the Ministry of Justice, the regulations are in accordance with the CPDPL, its revision and considering with the data protection principles enshrined by the OECD Guidelines, the Data Protection Directive as well as the APEC Privacy Framework. Available at: < http://www.moj.gov.tw/public/Attachment/01217148162.pdf>, accessed 19th March, 2011.

personal data in effect, particularly the right to privacy,.[193] In response to these criticisms as well as the demand of bridging the gap between technology developments and the lag of data protection laws, the Legislative Yuan issued a revision in 2010: the Personal Data Protection Law (PDPL).[194]

Purpose and objective

The PDPL aims to govern the collection, processing and use of 'personal information'[195] so as to prevent infringement upon *the right to personality*. The right to privacy has not been specifically mentioned here. In fact, the legal status of the right to privacy in Taiwan, in particular the relationships between *human dignity*, *the right to personality* and *the right to privacy* remain quite confusing.

'*The right of personality* is indispensable in guarding the individuality and free development of character, closely related to the safeguarding of *human dignity*, and is therefore protected by Article 22 of the Constitution'[196] (emphasis added).

'The detention of a criminal defendant not only will create a serious psychological impact upon her, but will largely affect her rights of personality such as *reputation, credit, and so forth* as well'[197] (emphasis added).

---

[193] Wen-Tsong Chiou, 'Comments on the Framework Problems of the Draft of Computer-Processed Personal Data Protection Law from the Perspective of the Conceptual Distinction between Information Self-determination and Information Privacy' (2009) 168 The Taiwan Law Review 172-174. Ching-Yi Liu, 'Not So Improved: Initial Commentry on the Personal Data Protection Law' (2010) 183 The Taiwan Law Review 147.

[194] According to Article 55 of the PDPL, the law will only become effective when the Executive Yuan (the central government administrative authority) issues an official order that specifies its effective date.

[195] The official translation of the PDPL (in English) does not distinguish different ideas between personal data and personal information. The title of the PDPL, for example, is translated as the 'Personal Information Protection Act'. This error has repeatedly been made through the whole official English translation of the PDPL. See: < http://law.moj.gov.tw/Eng/LawClass/LawAll.aspx?PCode=I0050021 > accessed 24th April, 2011.

[196] J. Y. Interpretation No. 664.

[197] J. Y. Interpretation No. 665.

Here, according to the former Honourable Justice Tze-Chien Wang, the right to privacy is included in the concept of the right to personality.[198] In other words, the right to privacy is merely *one* of the rights/ interests protected by the PDPL: the purpose of the PDPL is to protect the right of personality in relation to the *collection, processing and utilisation of personal data*.

It is essential to note that the interests protected by the PDPL must *not* be confused with the protection of personal data. This is because 'the concept of the right to privacy is much broader than the individual's right to protection of personal data,' and 'protection of personal data' could be considered as a particular type of the right to privacy.[199] This is also true in Taiwan, as Ding-Wang Lu, the Vice Director of the Department of Legal Affairs of the Ministry of Justice, in an academic article commenting the PDPL, argues that 'protection of personal data is exactly subject to the right to personality'[200] This is also implied by the J. Y. Interpretation No. 603.[201]

In sum, the PDPL protects the right to personality as well as human dignity, which covers the right to privacy and the right of data protection.

However, it can be misleading to refer the PDPL as the legislation to *merely* regulate the right to privacy. In fact, the term 'data protection' is often confused with 'privacy protection.' For example, in their popular contribution, Solove and Schwartz put that '[i]t is worth noting that the phrase "data protection" is frequently used to

[198] Tze-Chien Wang, 'The Issue and the Development of Protecting the Right to Personality (III): the Materialization of the Right to Personality and Its Scope' (2007) 97 Taiwan Law Journal 36.
[199] Mette Hartlev, 'The Concept of Privacy: An Analysis of the EU Directive on the Protection of Personal Data' in Deryck Beyleveld and others (eds), *The Data Protection Directive and Medicial Research Across Europe* (Ashgete Publishing 2004) 25.
[200] Ding-Wang Lu, 'Brief Commentary on the Amendment of Personal Data Protection Law' (2010) 183 The Taiwan Law Review 131.
[201] Ibid 131.

describe privacy protection in the European context.'[202] Nevertheless, as the PDPL (as well as the Data Protection Directive) considers the right to personality, which includes the fundamental rights and freedoms enshrined in the Constitution, to the extent that they may be interfered with in the use of personal data rather than only to protect privacy,' it is important to be clear about this.[203]

Definition and Scope

By reading the change of the title of the law in the amendment, it is easy to realise that the scope of the PDPL has been expanded: the definition of personal data is no longer limited to those 'computer-processed' data but *any* data format covering the information based on the possibility to identify someone whose identity is unknown when collecting his data.[204]

Moreover, unlike the CPDPL which limited its applications to the public sector and eight specified private sector areas,[205] the PDPL covers *all* industries and individuals as well as the public sector. This is now in line with the European context because, as the Ministry of Justice stated, it takes the European and international data protection legal regime into consideration.[206]

Data Protection Principles

---

[202] Solove and Schwartz 996.
[203] In terms of the Data Protection Directive, see: Beyleveld, 'An Overview of Directive 95/46/EC in Relation to Medical Research' 6.
[204] According to paragraph 1, Article 2 of the PDPL, personal data refers to ' a nature person's name, date of birth, national unified ID card number, passport number, characteristics, fingerprint, marital status, family, education, occupation, medical history, medical treatment, genetic information, sex life, health examination, prior criminal records, contact information, financial status, and social activities as well as other data which can be used directly or indirectly to identify the person.'
[205] These eight industries are: credit search businesses and groups or individuals whose major line of business is to collect or process personal data by computers, hospitals, schools, telecommunication, financial, securities, insurance, and mass communications industries.
[206] See: http://www.moj.gov.tw/public/Attachment/01217148162.pdf, accessed 1st June 2011.

The PDPL lays down some basic personal data protection principles which *correspond to* the Data Protection Directive. The personal data must be, namely:

1. processed fairly and lawfully (principle of *bona fide*, Article 5);
2. collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes (Article 5);
3. adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed (Articles 5, 11, 15, 16, 19 and 20);
4. accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified (Article 11);
5. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed (Article 11).

Data Controller's Duties: Transparency Demands/ Data Subject's Rights

During the legislating process of the amendment, there were public concerns on the balance between the right of personal data protection and the freedom of expression with respect to the media, political commentators and elected representatives. These worries stemmed from the legal obligation of the data controllers (including both government and non-government agencies) to inform data subjects (required by Article 9[207]) and obtain their prior explicit consent[208] before

[207] Article 9 states: 'A government agency or non-government agency should notify the data subject of the source of information and Item 1 to 5 of Paragraph 1 of the preceding Article, before processing or using personal information collected in accordance with Article 15 or 19 which was not provided by the data subject...'

[208] The PDPL requires a written consent under Articles 19 and 20.

collecting or publicising any information about them under Articles 19 and 20 of the PDPL.

With respect to the duty to inform of the data controller, such a rule seems to put considerable emphasis on the transparency demands and can be loosely thought as the data subject's right. However, in order to respond to the great public fear and the local legal ideology towards freedom of expression, which is rooted in the profound shadow of the leadership of Chiang Kai-Shek and the Nationalist Party during the *White Terror*[209] period, the reports of media are exempt from the rule due to the 'public interests' under Article 9.[210]

Nevertheless, this exemption could give rise to further concerns regarding obtaining valid consent.[211] This is because, apart from free will, a data subject's right to information which assures relevant knowledge and understanding is the fundamental precondition to give valid consent.[212] In this respect, the whole map of consent rules of the PDPL needs to be further examined.

Consent in the Data Protection Principles: the Procedure Justification

Rules provided by Articles 6, 16 and 19 of the PDPL raise some consent concerns. To understand and deal with the issue, it is better to start from the legislation

[209] The 'White Terror' describes a period of political suppression enacted by the Nationalist party under the leadership of Chiang Kai-shek. It was first enacted in 1947 as a result of the 228 Incident in Taiwan. During the period, the right of freedom of expression and press was strictly limited / banned by the longest martial law in the world (from May 19, 1949 to July 15, 1987).

[210] It states: '…The notification mentioned in the preceding Paragraph may not be given for the followings:…5: Personal data collected by the mass media for the purpose of news reporting on the basis of public interests…'

[211] The Taiwan Association for Human Rights (TAHR), for example, argues that the amendment allows too many exceptions from obtaining consent. See: Iok-sin Loa, 'Groups Decry Revision of Data Act' *Taipei Times* (Taipei, 29th April 2010) 3 <http://www.taipeitimes.com/News/taiwan/archives/2010/04/29/2003471758> accessed 22 March, 2011.

[212] For further discussions, see: Deryck Beyleveld and Roger Brownsword, *Consent in the Law* (Hart Publishing 2007) 145-153.

governing the prohibition of collecting and processing personal sensitive data.

Unlike the former CPDPL's lack of rules governing specific kinds of personal data, sensitive personal data, in principle, is not allowed to be collected, processed, as well as used under Article 6 of the PDPL. This is in line with Article 8 of the Data Protection Directive regarding the special categories of processing personal data. Under the PDPL, the sensitive personal data is defined as *medical treatment, genetic information, sex life, health examination and criminal record*. There are four exemptions, namely:

1. in accordance with law;
2. it is necessary for the government agency to perform its duties or for the non-government agency to fulfil the legal obligation, and when there are proper security measures;
3. the data subject has disclosed such information by himself, or when the data concerned has been publicized legally; and
4. the personal data is collected, processed or used under certain methods by a government agency or an academic research institution based on the purpose of medical treatment, personal hygiene or crime prevention statistics and/or study.

These four items thus can be viewed as the *substantive* justifications when balancing competing interests. In this regard, prohibited actions may be permitted with conditions. Surprisingly, unlike Article 8(1) of the Data Protection Directive, readers cannot find a procedural justification of the explicit consent under Article 6 of the PDPL. Therefore, in reading its text literally, it might invite the interpretation that if any individual, group or the government meet any of the above exemptions, the

sensitive personal data discussed can be collected and processed *without* consent.

What is the role of consent then? Is consent not a sufficient, or necessary (procedural) justification in such circumstances? This generates a problem of the lack of clear guidance, or misinterpretation that consent may not even have any place in sensitive data collection and processing behaviours. This has been criticised by Taiwanese academics by looking at the framework of Formosan personal data protection law.[213] We shall review this problem in the next chapter.

Proportionality in the Data Protection Principles: the Substantive Justifications

The fairly vague and flexible language of the definition and scope of public interests and proper reasons/ reasonable expectations exemptions under Articles 6, 9, 19, and 20 of the PDPL are further criticised as leaving loopholes for data controllers to substantively justify the collection and processing of personal data.[214] The open-list nature of public interests, for example, makes it 'potentially compatible with any moral theory, though the identification of relevant public interests and the method of weighing competing interests will differ from one theory to another.'[215] To deal with the 'public interests' justification, on the basis of the PGC grounds, three classes of reasons can be legitimately applied as guidelines:[216]

1. Instruments in order to secure respect for the rights of fellow agents in the community;[217]

[213] Chiou (n 193) 181-186. Liu, 'Not So Improved: Initial Commentry on the Personal Data Protection Law' (n 193) 151.
[214] Liu, 'Not So Improved: Initial Commentry on the Personal Data Protection Law' (n 193) 156-162. Chiou (n 193) 181-186.
[215] Beyleveld and Pattinson, 'Confidentiality and Data Protection' (n 179) 666.
[216] Beyleveld and Brownsword, *Consent in the Law* (n 212) 271-272.
[217] This covers three sub-categories: '(1) interventions that are designed to discourage violations of rights; (2) interventions that aim to co-ordinate the community's activities to that responsibilities to right-holders are discharged more effectively; and (3) interventions that are designed to assist with the

2. Instruments in order to preserve the context in which autonomous agents will enjoy the opportunity to flourish as members of a community committed to human rights and responsibilities;[218] and

3. Instruments in order to give effect to prohibitions that have been expressly authorised by members of the community.

As regards the third category, it should be noted that, since Taiwan is simply not a considerably small community like an ancient Greek city-state, it is not practical to apply such guidelines.[219] Overall, as the national critics hold, given the open textured nature of the language, the abuse of such exemptions in the name of 'public interest' should not be viewed as a blank cheque. Also, the applied instruments should take the criterion of degrees of needfulness for action into account. This shall be further discussed in section 6.4.2.

Institutional Frameworks

It has been argued that, under the European data protection tradition, an independent and specialised supervisory agency dealing with the data protection framework has been assumed to be best suited (or, essential) to ensure the full implementation of such rules in practice.[220]

Although the PDPL seems to draw from European experiences, particularly the

---

enforcement of rights.' Ibid 271.

[218] This category also covers three sub-categories: '(1) interventions that are designed to make essential community choices between morally optional conduct or forms of life; (2) interventions that provisionally settle the community's position on a morally contested matter (whether relating to the interpretation of rights principles or their application); and (3) interventions that aim to preserve those features of the context from which agents take their identity as members of a community committed to respect for rights, and concomitantly, their responsibilities.' Ibid 271-272.

[219] Ibid 357.

[220] Peter Blume, 'Transbroder Data Flow: Is There a Solution in Sight?' (2000) 8 International Journal of Law and Information Technology67. Also, Lingjie Kong, 'Enacting China's Data Protection Act' (2010) 18 International Journal of Law and Information Technology 225.

Data Protection Directive, there is, surprisingly, *no* single/ independent supervisory authority in charge. Instead of having an independent oversight body, the enforcement of the PDPL is left to the Ministries responsible for each industry sector. By reading Articles 53[221] and 55,[222] however, it is arguable that the Ministry of Justice acts as the supervisory body, or at least the chief authority in charge of the PDPL and the data protection institutional framework. Nevertheless, unless it is clearly appointed by the law, the Ministry cannot always play multiple roles as the *de facto* promoter, guardian, and defender of the PDPL regime. For example, the Ministry may not be able to defend individuals against the public authorities' wrongdoings in relation to the right to privacy since the Ministry itself is the executive department under the Executive Yuan rather than an independent authority. This is thus quite reasonable for the local commentators to share a general opinion that, although evidence of the enforcement or effectiveness of the data protection law is lacking, the PDPL (as well as the CPDPL) is ineffective.

5.4 The Concepts of the Right to Privacy in Taiwan

Building upon the knowledge of the status quo of the Formosan privacy framework, the categorisation offered by Allen, i.e., spatial privacy, decisional privacy, and information privacy, will be used for later discussion.[223] This categorisation is followed by a majority of Formosan commentators, including the former Honourable

[221] Article 53 of the PDPL states: 'The specific purpose and the classification of personal information stipulated in this Law should be prescribed by the Ministry of Justice in conjunction with the government authority in charge of subject industry at the central government level.'
[222] Article 55 of the PDPL states: 'The Enforcement Rule of this Act shall be prescribed by the Ministry of Justice.'
[223] The reasons of the general application of Allen's categorisation have been provided in section 4.3.2.

Justice Tzu-Yi Lin,[224] who is one of leading scholars in the Formosan privacy law field. Moreover, by reading J. Y. Interpretation No. 603:

> Although the right of privacy is not among those rights specifically enumerated in the Constitution, it should nonetheless be considered as an indispensable fundamental right and thus protected under Article 22 of the Constitution for purposes of *preserving human dignity, individuality and moral integrity*, as well as *preventing invasions of intimacy of private life* and *maintaining self-control of personal information* (See J. Y. Interpretation No. 585)… (emphasis added)

three dimensions of privacy can as well be distinguished: (1) individuality and moral integrity can be argued as referring to spatial privacy; (2) preventing invasions of intimacy of private life implies the concepts of decisional privacy; and (3) maintaining self-control of personal information indicates informational privacy. To understand Taiwan's current privacy discussions, it is an appropriate and effective way to apply the general categorisation given by Allen.[225]

However, there is a need to make a distinct between Professor Allen's proposal and this thesis. As previously addressed in section 4.2.2, Allen's view on privacy is based on a duty-based consideration. This thesis, on the other hand, applies the Gewirthian theory subject to a right-based thinking. An agent must be granted generic rights for any purpose it has voluntarily chosen. Only by this premise the generic rights of others will not be threatened under a right-based line of reasoning. Undesired access by any other agent over the agent's personhood thus causes a generic harm (although it may be justified under the PGC). To violate this generic need (privacy) through an actual *physical* admission to spaces or body integrity is termed the spatial

[224] Lin (n 167) 700-701.
[225] See: section 4.3.2.

privacy harm. *Metaphorical* access to the agent's personhood in the sense of possibilities for intruding and intervening in a voluntarily act is termed decisional privacy, while in the sense of access to information is termed as informational privacy.[226]

5.4.1 Spatial Privacy

The right to spatial privacy refers to the right to respect and protect the interest of an individual's body integrity and the space where the individual lives or stays. It embraces the prevention against interferences with: (1) physical and mental integrity; (2) limited access on private space and communication; and (3) the living space and environment.

First, an individual's body concerns not only the most intimate aspect of one's private life,[227] but also the ability to keep oneself from unwanted access by others. Both interests are core concepts of the right to privacy. Under Article 8 of the Constitution, which states that 'personal freedom shall be guaranteed to the people,' the right to be free from interference with *physical and psychological integrity* is protected.

With respect to physical integrity, the avoidance of *non-consensual physical assault of the body*, for example, can be identified as falling within this form of privacy: individuals are protected against assaults by public bodies, in particular by the police, prosecution, and judicial powers.[228] J. Y. Interpretation No. 535, for

[226] See also: Beate Rössler, *The value of privacy* (Polity Press 2005) 43-44.
[227] This opinion is also stated by the ECtHR. See for example: *Y.F. v Turkey* (App no 24209/94) ECHR 2003-IX, para. 33.
[228] Article 8 of the Formosan Constitution states that: 'Personal freedom shall be guaranteed to the

instance, states that

> According to Article 11, Clause 3, of said Act (The Police Service Act), a police check is authorized as a way for police to facilitate law enforcement. However, the ways in which police checks are conducted including searches, street checks, and interrogations may have a great effect upon *personal freedom*, right to travel, property right and *the right to privacy* and therefore such checks must be in accordance with the rule of law as well as legal principles guiding police functions and legal enforcement. (emphasis added)

The Honourable Judges agree that the (stop and) search cases by the police can lead to potential violations of privacy. Physical assault could as well affect mental integrity since it may provoke emotions experienced in anticipation of such harm. Similarly, the *non-consensual exposure of the body* not only violates physical integrity, but also leads to a breach of one's mental equilibrium. Clear examples can be found in the use of X-ray, ultra red-ray or electromagnetic waves to assess persons for security (or any other) reasons that can interfere with body integrity since unnecessary exposure in front of others (when the individual is aware of such scan), or having one's body scrutinised without knowing (i.e. when the individual is unaware of such scan) that

---

people. Except in case of *flagrante delicto* as provided by law, no person shall be arrested or detained otherwise than by a judicial or a police organ in accordance with the procedure prescribed by law. No person shall be tried or punished otherwise than by a law court in accordance with the procedure prescribed by law. Any arrest, detention, trial, or punishment which is not in accordance with the procedure prescribed by law may be resisted.
When a person is arrested or detained on suspicion of having committed a crime, the organ making the arrest or detention shall in writing inform the said person, and his designated relative or friend, of the grounds for his arrest or detention, and shall, within 24 hours, turn him over to a competent court for trial. The said person, or any other person, may petition the competent court that a writ be served within 24 hours on the organ making the arrest for the surrender of the said person for trial.
The court shall not reject the petition mentioned in the preceding paragraph, nor shall it order the organ concerned to make an investigation and report first. The organ concerned shall not refuse to execute, or delay in executing, the writ of the court for the surrender of the said person for trial.
When a person is unlawfully arrested or detained by any organ, he or any other person may petition the court for an investigation. The court shall not reject such a petition, and shall, within 24 hours, investigate the action of the organ concerned and deal with the matter in accordance with law.'

lead to stigma which may damage mental well-being.

To maintain bodily integrity, *the right to be let alone* and *the right not to be spied on* in the restricted access space regarding the human body should also be taken into account. This is particularly crucial with respect to mental integrity. *Unwanted* watching, listening, taking of photographs, recording or any observations of an individual's body and behaviour, will interfere with the individual's interests in bodily integrity. Article 23 of the 1996 Radio and Television Act and Articles 315-1 and 315-2 of the Criminal code, for example, specifically focus on these interests. To complete, it must be added that those two forms of body integrity– *physical and psychological integrity* are not separated, but that there is a certain degree of overlap.

Secondly, *private* spaces such as living, working, studying or entertaining spaces of an individual are as well within the category of protecting spatial privacy. The limited access of visible, tangible, or touchable spaces as well as the realms of life and the way of life of an individual is protected.[229] This is enshrined by Article 10 of the Constitution which declares that individuals shall have freedom of residence and of change of residence. Moreover, Article 12 of the Constitution which stands for the freedom of privacy of correspondence can be argued as contributing to the protection of intangible private space.

The right to be not spied on in private spaces and communications is of central importance under this sub-category. Regulations on surveillance can reflect the balance between this interest and other rights and freedoms. It is held, for example, in J. Y. Interpretation No. 631:

> The Communication Protection and Monitoring Law is a statute enacted by the State

[229] Rössler (n 226) 142.

> for the purpose of balancing the conflict of interests between "protection of the people's freedom of privacy of correspondence from illegal invasion" and "guarantee of national security and maintenance of social order." (see Article 1 of the Communication Protection and Monitoring Law) According to its provisions, only where it is necessary to safeguard national security and maintain social order the State may issue the writs of communication monitoring to examine the people's private correspondence, provided that both substantive and procedural legal requirements are met. (see Articles 2, 5 and 7 of the Communication Protection and Monitoring Law)

As regards the limited access related to physical separation or isolation from others, in J. Y. Interpretation No. 535 concerning the police check, it is provided that it must be protected to the same extent as residence under Article 10 of the Constitution if the police check is exercised in the private spaces.

Thirdly, the protection of the private *space* itself should also be taken into account. This is because without such a private 'space,' individuals are not able to act privately. The protection of this interest is closely related to the property right under Article 15 of the constitution which states that 'the right of property shall be guaranteed to the people.' Therefore, the property right to home as a shelter is crucial to achieve and maintain the right to privacy. Moreover, the maintenance of such a space, e.g., the protection of one's living and life-supporting environment is also a necessary interest/ requirement to guarantee the spatial privacy. Lastly, as regards the environmental right, the Constitution does not mention it in the main text. However, it is stated by Article 10(II) of the Additional Articles of the Taiwan's Constitution that '[e]nvironmental and ecological protection shall be given equal consideration with economic and technological development.'

5.4.2 Decisional Privacy

Professor Allen proposes a second category of privacy – decisional privacy, concerning with 'freedom from governmental or other outside interference with decision-making and conduct, especially respecting appropriately private affairs.'[230] Following her reasoning, this dimension expresses the concept of privacy in a liberty sense.[231] Briefly, this dimension refers to action that is simply classified as a private matter because it is no one else's business other than the agent at issue.[232]

Decisional privacy cannot be clearly identified in Taiwan's Constitution. However, according to Article 13 of the Constitution stating that individuals shall have the *freedom of religious belief*, an individual's 'own business' concerning her intimate aspect of personhood to voluntarily choose her religious belief is guaranteed. In this regard, merely choosing one's religious belief normally will not violate others' generic conditions of agency, as it could be done alone without having any form of relationships with others. This article thus can be viewed as a reflection of decisional privacy.

However, it should be noted that not all social behaviour and actions can be done alone without establishing and affecting relationships with others – as there is no ultimate private/ isolate space for an agent to do things without encountering others. *The right to decide whether or not and how to develop relationships with other human beings* concerns an individual's personhood, particularly if it comes to the decision to

[230] Anita Allen, 'Taking Liberties: Privacy, Private Choice, and Social Contract Theory.' (1987) 56 Cincinnate Law Review 465-466.
[231] Ibid 465-466. In the essay she remarks, Allen does not clearly distinguished between liberal, freedom, and decisional privacy. For a discussion in a greater detail, see, e.g., Rössler (n 226) 79-110.
[232] Rössler (n 226) 79.

maintain or to end familial and other intimate relationships. In J. Y. Interpretation No. 554, in applying Article 239 of the Criminal Code relating to a person who commits adultery and to the other party in the adultery that are punishable, the constitutional court holds that

> Marriage and family serve as the foundation on which our society takes its shape and develops and are thus institutionally protected by the Constitution (See Interpretations Nos. 362 and 552). The root of our marriage system lies in the freedom of personality, *with such social functions as the maintenance of the order of human relationships* and gender equality, and the raising of children. (emphasis added)

In this case the Court considered that 'the cornerstone supporting matrimonial cohabitation is unquestionably the relationship between the husband and wife established upon the affection and faithfulness toward each other,' and it is the 'affection between the husband and the wife and their *privacy*' that should be centrally taken into account when dealing with the relationship of the marriage.[233] (emphasis added) It thus arguable that the Court recognises that decisional privacy has to be considered since the marriage involves intimacy between husband and wife (or any intimate partners).

Additionally, the same case contemplates the *freedom of sexual activity*. It is held that 'the freedom of sexual behaviour is inseparably related with the personality of individuals, and every person is free to *decide* whether or not and with whom to have sexual affairs.' (emphasis added) On this basis, the Honourable Justices confirmed that the right to establish and develop sexual relationships with other human beings is

[233] Paragraph 3 of the reasoning of J. Y. Interpretation No. 554.

closely related to decisional privacy and thus should not be violated by others.

As a type of decisional privacy, furthermore, the *right to retain and choose one's name* is also protected. It is held by J. Y. Interpretation No. 399 that

> The right of an individual to select his/her own name is a type of personal right. *The name of an individual signifies an aspect of his/her personality.* Therefore, the right to *choose* one's own name is a physical freedom safeguarded under Article 22 of the Constitution… (emphasis added)
>
> …Whether or not the characters chosen in giving names are decent hinges upon the subjective value judgment of the person who enjoys the right to a name, such naming process deserves deference from the agency-in-charge in making its own decisions thereof.

5.4.3 Informational Privacy

The notion under the broad rubric of informational privacy can be roughly understood as closely related to 'control over what other people can *know* about oneself.'[234] The value of this dimension of privacy is quite similar to decisional privacy in the sense of personal integrity and autonomy and overlaps with spatial privacy, particularly bodily integrity and limited access to private spaces and communication,[235] yet it is particularly manifest in *informational aspects* concerning one's *own private life*.[236]

[234] Rössler (n 226) 111.
[235] N. A. Moreham, 'The Right to Respect for Private Life in the European Convention on Human Rights: a Re-examination' (2008) 1 EHRLR 62-63.
[236] Roger Brownsword, 'Consent in Data Protection Law: Privacy, Fair Processing and Confidentiality' in Serge Gutwirth and others (eds), *Reinventing Data Protection?* (Springer 2009) 93.

A first reading of the definition of informational privacy might be associated with the idea of the right to protect personal data, in particular the requirement of fair processing under such a right. However, there is a need to untangle the right to informational privacy from the right to protect personal data.[237]

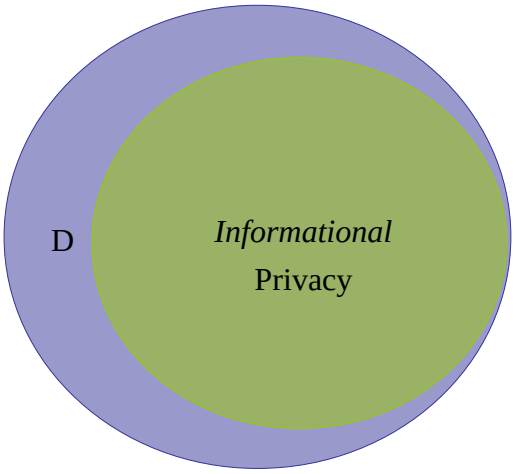


Figure 5.1: The PDPL: the right to informational privacy and the right to protect personal data.

First, not every type of information relating to an agent is covered under the scope of informational privacy. Public knowledge, for example, is excluded from private information. This is because the right to informational privacy protects *private* information and if the information has been publicised, such information is simply no longer private information.[238] This type of personal data has been placed in Article 19.3 of the PDPL as an exemption to collecting and processing personal data.[239]

Secondly, with respect to the right to protect personal data (D shown in figure 5.1), as previously argued, the PDPL aims to protect fundamental rights and freedoms *to the extent that they may be violated in the collection, process and use of personal*

[237] See: ibid 93-96.
[238] Neil C. Manson and Onora O'Neill, *Rethinking Informed Consent in Bioethics* (CUP 2007) 103.
[239] Article 19.3 of the PDPL: "Except the information stated in Paragraph 1 of Article 6, the non-government agency should not collect or process personal information unless there is a specific purpose and should comply with one of the following conditions: …3. Where the Party has disclosed such information by himself or when the information has been publicized legally; …"

data. Moreover, it is arguable that the scope of data is broader than information since information is simply processed data that has a specific meaning for the person who receives it.[240] By recognising this, the thesis shares the Brownsword's view to 'treat personal data as a broad class of information'[241] that relates to the data subject. However, it must be noted that informational privacy is merely a type of privacy.

The idea of informational privacy has not been widely discussed before the information technology reached an advanced and mature level. In Taiwan, informational privacy was first mentioned by the constitutional court in J.Y. Interpretation No. 293 that:

> This provision[242] was enacted to protect bank customers' confidential information on their individual properties and to prevent banks from freely and unilaterally disclosing such information, with a view to protect the people's right of privacy.

Yet this constitutional interpretation in relation to the *right to personal financial/ property informational privacy* did not clearly explore the concept of informational privacy. Neither did the later constitutional interpretation (J.Y. Interpretation No. 586) concerning the same type of right offer any indication of the concept of informational privacy.[243] A general concept of information privacy was dealt with by J.Y. Interpretation No. 603:

---

[240] Patricia Margaret Alexander, 'Towards reconstructing meaning when text is communicated electronically' (PhD thesis, University of Pretoria 2002) 66, available at: <http://upetd.up.ac.za/thesis/available/etd-08192002-155431/unrestricted/03chapter3.pdf> accessed 14 January 2012.

[241] Brownsword, 'Consent in Data Protection Law: Privacy, Fair Processing and Confidentiality' 95.

[242] Article 48, Paragraph 2, of the Banking Act stipulates: "Unless other laws or regulations promulgated by the central governing authority indicate otherwise, banks shall keep their customers' information regarding deposits, loans and remittances in strictest confidence."

[243] J.Y. Interpretation No. 586 merely mentioned that 'Because the creation of filing obligations places a restriction on the people's constitutionally guaranteed autonomous right to information and property right, it shall be imposed by law instead of by administrative regulations.'

> As far as the right of information privacy is concerned, which regards the self-control of personal information, it is intended to guarantee that the people have the *right to decide whether or not to disclose their personal information*, and, if so, to what extent, at what time, in what manner and to what people such information will be disclosed. It is also designed to guarantee that the people have *the right to know and control how their personal information will be used*, as well as *the right to correct any inaccurate entries contained in their information*. (emphasis added)

Hence three sub-categories of rights under this dimension can be distinguished, namely:

1. The right to decide/ consent whether or not to disclose information;
2. The right to know and control how their personal information will be used; and
3. The right to correct any inaccurate entries contained in their information.

All of the above rights are closely related to the autonomy-oriented aspects as well as to the perspective of *bodily integrity* which emphasises the protection of personality.[244] The first type of right emphasises an individual's consent to disclose her personal information, which considerably influences on the collection, retention, and processing of such information. Furthermore, it encompasses fundamental data protection principles in relation to the disclosure of personal information. This right also covers the *right to objection*.

The second right is the *right to access and to be informed*, which is, as Hartlev points out, a prerequisite for the individual to 'be able to take part in the control of the

[244] The understandings of the concepts of information privacy here under J. Y. Interpretation No. 603 are mainly based on Mette Hartlev's contribution. See: Hartlev (n 199) 29.

flow of information, and to know for what purpose information about him/her will be processed.'[245] The last right is the *right of correction*, which supports individuals to control their information.

5.5 Data Protection Issues Raised by the Biometric and RFID Technologies

Having introduced some essential information on biometric and RFID systems and their omnipresence in people's everyday lives, outlined both the European and Formosan data protection legal regimes, and examined the concepts of privacy, I am now able to identify a number of issues for later discussions on the basis of the legal issues highlighted so far,.

The leading question requiring consideration is whether there is a right to benefit from the technologies discussed here, and if so, to what extent it should be taken into account. Another inevitably following issue focuses on data protection concerns, in particular the right to privacy, brought by the aforementioned technologies. This invites a number of discussions concentrating on the concept of the right to privacy. The first issue rests on the assessment of the rights that are covered (by the right to privacy in both legal regimes). It then needs to be asked which of these are generic conditions and at what level. This is the precondition to answer the subsequent questions about the priority of the rights. Secondly, the question closely related to the application of technologies at stake is the claim that 'if you have got nothing to hide, you have nothing to fear/ lose' (the 'nothing to hide' argument). How to assess the validity of this argument? Thirdly, how can the development of technology affect the

[245] Ibid 30.

right to privacy, in particular the right to information privacy? Furthermore, how to deal with the changing concept of information privacy, which is profoundly affected by the development of technology, and its applications?

Moreover, since there are only a few absolute rights (and apparently, the right to privacy, the right to protection of personal data,[246] and the right to benefits from technology are not considered to be absolute rights), most of the fundamental rights and freedom may be overridden in specific conflicting cases. This has already been shown by examining the exceptions to the right to privacy in both legal regimes. This gives rise to the central question of this thesis – how to deal with the competing rights (the right to benefit from technology and the right to privacy for example) when they are in a conflict?

Two justifications are involved when considering this question. The first one is the procedure justification – consent. We have seen that consent indeed plays a crucial role in the data protection principles in both legal regimes; however, we should neither undervalue nor overvalue it. On the other hand, there is a second possibility of the justification – the substantive justifications to reconcile the competing interests and rights. The principle of proportionality has been taken into account in both legal systems considered here. Is such a principle able to play a distinct role? If not, is there a criterion approaching the question of reconciling competing rights and interests? How to apply such a criterion?

One crucial question that remains unanswered is whether conflicts between the right to privacy and the right to benefit from advances in science and technology can be avoided. It seems that although there can be applicable criteria to deal with the

[246] Court of Justice of the EU, judgment of 9112010, Joined Cases C-92/09 and C-93/09 Volker und Markus Schecke and Eifert [2010] ECR I-0000.

conflicts, it is much better to avoid such conflicts. In other words, it is mistaken to always regard the competing rights respecting *the developing technologies within a data protection law regime* as belonging to two mutually exclusive sets.

I will discuss these questions on the basis of the PGC architecture.

Chapter 6

Privacy and Data Protection Issues related to Biometric and RFID Technologies

6.1 Introduction

This Chapter offers a commentary on the privacy and data protection issues regarding the technologies discussed here through the lens of the PGC. As addressed in the last chapter, the first issue to examine will rest upon the question of whether there is a right to benefit from the advances in science and technology in light of the PGC. If so, how should we treat it? I will then turn to the fears provoked by biometric and RFID technologies. Previously, I have recognised that the primary consideration with respect to these new technologies and their implications is the worries about their impact on privacy and data protection. Sections 6.3 and 6.4 will address these privacy and data protection questions.

Before evaluating these issues, however, a preliminary question has to be answered: as we have seen in section 4.3.1, the ECHR is in line with the PGC; but how about the Taiwanese legal regime? More specifically, do the human rights values employed by the Formosan Constitution satisfy all the features of generic rights by which the PGC can be viewed as a necessary criterion of legal validity?

By applying the dialectically necessary method to the concept of agency, the PGC has been justified as the basic principle of human rights *in any community*, requiring agents to act in accordance with the generic rights of all agents. There are some observations to be made on the Formosan situation. First, the immediate acceptance of

the PGC follows that all agents should be treated equally for a purpose, whatever that purpose is. On the basis of the alternative justification addressed in section 3.4, the acceptance of the impartiality assumption is of central importance. In this regard, the Formosan Constitution addresses equality in Articles 7 and 5.[1] Moreover, although, Taiwan is not currently a member of the UN, the Act to Implement the International Covenant on Civil and Political Rights and the International Covenant on Economic, Social and Cultural Rights has been promulgated on 22nd April, 2009.[2] Accordingly, the contingency upon which the dialectically contingent approach relies, namely, the requirement of the acceptance of *human rights* to be *equally* held by *all* recipients/ agents has been recognised.

Secondly, it has been repeatedly confirmed by the Constitutional Court that the government should grant both negative and positive rights. With reference to the right to privacy, the Constitutional Court identified it as a fundamental right covered by the scope of Article 22 of the Constitution, which requires the government to stay out of citizen's business. As regards the obligations of the government, the Constitutional Court also requires the government authorities to provide both organisational and procedural privacy-enhanced entitlements.[3]

Thirdly, the Constitutional Court considers that the core value of Taiwan's Constitution is to protect human dignity and to respect the 'free development of personality.'[4] The idea of 'human dignity' is a basic requirement of the agency since

[1] Article 7 states that 'All citizens of the Republic of China (Taiwan), irrespective of sex, religion, race, class, or party affiliation, shall be equal before the law.' Article 5 declares that 'There shall be equality among the various racial groups in the Republic of China (Taiwan).'
[2] Article 2 states that '[h]uman rights protection provisions in the two Covenants have domestic legal status.'
[3] See J. Y. Interpretation No. 603.
[4] See J. Y. Interpretation Nos. 603 and 613.

'dignity as the basis of rights is constituted by the property of being an agent'.[5] Violating an agent's dignity is the ultimate prohibition of the PGC since it is to act contrary to the agent's agency granted by the PGC. However, it must be noted that the concepts of 'human dignity' held by the Constitutional Court are still quite vague.[6] This is partly because the concepts of human dignity are profoundly affected by traditional Confucianism and the Han culture, which pre-date modern constitutionalism.[7] Nevertheless, there is no doubt that human dignity is acknowledged as the core value of the Constitution.

However, this is not the whole story: it is, 'actually by virtue of *vulnerable* agency that the generic rights are to be granted.'[8] The second core value, i.e., the free development of personality enshrined by the Constitution, is arguably in line with this. This is because, by protecting the free development of personality, the agents are capable of reflecting their own physical and mental integrities and frailties which 'constitute the dignity that ground the generic rights.'[9]

It is noted that an application and a competent decision-making body applying the PGC are essential when evaluating regulatory attempts.[10] The above examination seems to lead to an observation, at least *pro tanto*, that the constitutional approach followed by the Judicial Yuan can meet the requirement. It is thus now possible to proceed with the discussion.

---

[5] Deryck Beyleveld and Roger Brownsword, *Human Dignity in Bioethics and Biolaw* (OUP 2001) 112.
[6] See: Cheryl Saunders and others, 'Asian Constitutions in Comparative Perspectives' (2009) 4 National Taiwan University Law Review 203.
[7] Ibid 210-211.
[8] Beyleveld and Brownsword (n 5) 112.
[9] Ibid.
[10] Shaun D. Pattinson, *Influencing Traits Before Birth* (Ashgate Publishing 2002) 71.

6.2 The Right to Benefit from Advances in Science and Technology?

This section aims to examine whether there is a right to benefit from progress in science and technology. If so, is it a generic right on the basis of the PGC ground? As only a generic right may override another generic right (e.g., the right to privacy and data protection rights), this is a preliminary question for subsequent assessments of privacy and data protection issues related to the technologies at hand.

Indeed, the right to benefit from advances in science and technology is not in itself a new phenomenon. It has been recognised by relevant international human rights instruments, such as:[11]

1. Article 27 of the Universal Declaration of Human Rights (UDHR);[12]
2. Article 15(1)(b) of the International Covenant on Economic, Social and Cultural Rights (ICESCR); [13]
3. Article 13 of the American Declaration of the Rights and Duties of Man; [14]
4. Article 42 of the Arab Charter of 2004;[15] and
5. Article 14 of the Protocol of San Salvador to the American Convention on Human Rights of 1988.[16]

[11] See: Stephen Marks, 'Out of Obsecurity: the Right to Benefit from Advances in Science and Technology and Its Implications for Global Health' (The 3rd conference on Law, Science, and Technology: Health, Science, and Human Rights, Taipei, 18 December 2010) 13-14 < http://www.hsph.harvard.edu/faculty/stephen-marks/files/spm_taipei_18_dec_2010_keynote_address-_ver_feb_16_2011.pdf> accessed 3 August 2011. For the official statements of conferences held by international organs (such as the UNESCO), see: UNESCO, 'The Right to Enjoy the Benefits of Scientific Progress and its Applications' <http://unesdoc.unesco.org/images/0018/001855/185558e.pdf> accessed 3 August 2011, 17-18.
[12] It states that 'Everyone has the right freely … to share in scientific advancement and its benefits.'
[13] It reads the right: 'to enjoy the benefits of scientific progress and its applications.'
[14] It states as the right of every person 'to participate in the benefits that result from intellectual progress, especially scientific discoveries.'
[15] It expresses that 'Every person has the right … and to enjoy the benefits of scientific progress and its application.'
[16] It declares that "the right of everyone … To enjoy the benefits of scientific and technological progress as well as …the benefits to be derived from the encouragement and development of international cooperation and relations in the fields of science, arts and culture…"

Moreover, according to the *Venice Statement on the Right to Enjoy the Benefits of Scientific Progress and its Applications* issued by UNESCO in 2009, it is suggested that the obligations of the State in relation to this right involve not only the negative ones, but also the positive ones.[17]

In light of the PGC, this right, which includes vast technological fields, can be considered as a generic right. Several complex technologies, indeed, involve improvements with respect to an agent's capacities for successful action in general. They include, for example: (1) biotechnologies in medicine scope that affect the beginning of life, the quality and enjoyment of life, and the end of life; (2) the scientific advances in the area of food production, such as genetically modified agricultural products that may affect the human diet; and (3) the information, communication and identification technologies which increase opportunities for the improvement of capacities for action at all or general chances of successful action, such as life, education, access to accurate information and so forth.[18] Moreover, for those technologies and their applications which have been broadly and consistently used in the modern era, to interfere with their use is to diminish an agent's chance of achieving the agent's purpose, whatever the purposes being pursued. Hence, the technologies involved are/ might be things that are needed for making successful actions possible.

This is particularly important in considering that the implementation of generic rights requires other agents to effectively prevent generic harms and secure such rights. This duty for the agents can be more efficiently met by governments and is

[17] UNESCO (n 11) 17-18. Also, Marks (n 11) 17-19. However, it has to be noted that the obligations mentioned are not only focusing on the protection of the right to benefit from the progress of science and technology, but also the other competing fundamental rights and freedom.
[18] UNESCO (n 11) 13-14.

largely left to governments.[19] Hence, for example, the technologies focused on in this thesis – biometric and RFID technologies – are widely applied by the states and public authorities to improve collective rights.

From a Gewirthian perspective, this right involving the ongoing process of science and technology requires attention. Two issues are of particular relevance: first, the accessibility of benefits, and second, the relationship to other rights.[20]

1. The Accessibility of Benefits

Since the right to enjoy the benefits from the progress of science and technology is a generic right, all agents should, therefore, equally possess this generic condition of agency. To enjoy the right to benefit from the progress of science and technology, we must consider that such a right is as negative as it is positive. It is recalled that, as regards the positive rights under the PGC, other agents categorically ought to help an agent to secure the generic needs when she cannot do so by her own unassisted efforts *if she so wishes*. However, such positive rights to generic conditions of agency are in potential conflict with the other agents' generic rights. This is because they impose obligations to the other agents that limit the other agents' generic rights.[21] With respect to the right at hand, for example, the proposition of sharing in such benefits as a generic right of all agents greatly challenges the financial interests of researchers, researchers/inventors of science and technology, and even governments.[22] The patent and the surrounding intellectual property rights regarding the science and technology, thus, may be interfered with.

[19] Alan Gewirth, *The Community of Rights* (The University of Chicago Press 1996) 56.
[20] These two issues are identified and responded by the Venice Statement and the related conference held by UNESCO. See: UNESCO (n 11) 5.
[21] Gewirth (n 19) 44.
[22] Marks (n 11) 35.

There must be, therefore, an adequate framework, and an adequate moral or ethical justification, to deal with the market in order to reconcile competing rights: the right to enjoy the benefits of advances in science and technology and the right to (intellectual) property.[23] This issue, particularly in the field of the enjoyment of the benefits of biotechnology discussed in this thesis, inevitably raises a question in relation to the debate of market regulation. A brief overview of this debate may offer a glimpse of what is at stake.

On the one hand, it has been claimed that free markets are better suggested. This is because, based on a Utilitarian argument, this model may promote the overall utility as long as the deals between the agents are not harming anyone and the deals possess the potential of bringing mutual profits.[24] In a preference Utilitarian version, for example, it is the maximisation of the subjective preferences of agents in a calculus in which all preferences count equally.[25] Moreover, based on the Libertarian rights ethics, voluntary exchanges uphold the respect of individual liberty. Free markets are therefore advocated by such theories.[26]

On the other hand, there are objections to the above free-market model.[27] A general objection against the free-market model, for example, considers that technologies associated with human bodies are incompatible with human dignity. It can be, rather, argued that certain benefits and social practices cannot be the object of trade or patents. It has been argued, for instance, that it is inappropriate to patent processes or products involving tissues from human beings, are for it may be contrary

[23] It is noted that even in a free-market model, the market should still be attached by some instruments at a minimum level e.g., the contract obligations and tax.
[24] Michael J. Sandel, *Justice: What's the Right Thing to Do* (Penguin Books 2010) 75.
[25] Richard M. Hare, *Moral Thinking: Its Levels, Methods and Point* (OUP 1982). It is noted that preference utilitarianism pre-supposes that the strength of agent's preferences can be measured and compared on a scale. See: ibid Chapter 7.
[26] Sandel (n 24) 75.
[27] Ibid 81-91.

to human dignity.[28] Some regulations, according to such a consideration, incorporate a morality exclusion.[29] Moreover, a free-market model cannot avoid the possibility of an initial situation of inequality. It is debateable that not every deal is fair in a free market. This is because there are chances that the deal is made under a non-free or out-of-necessity situation. In such cases, even though there may be consent in attendance, it may still be made in an invalid way.[30] Overall, this objection is similar to the 'dignity as constraint' argument on a dignity-based perspective.[31]

A specific objection, furthermore, contends that the objects, i.e., the donors of human body tissues, were used as a mean rather than an end. This fails to recognise the holders of generic rights as agents. Therefore, this objection fits with the 'dignity as empowerment' argument.[32]

However, both objections are well founded in the PGC. First, to violate the PGC, there must be a harm interfering with the status of agency. It might be suggested that in certain cases, whether directly or indirectly, there might be a violation. However, since this is not true in every case, the answer should be left open. In other words, as Beyleveld and Brownsword remark, '[u]nless it is argued that patents on human genes impinge upon the status of agents as rights-bearers, there is no case to answer.'[33]

Secondly, unlike the duty-based reasoning, the PGC allows an agent to waive the benefits of generic rights under the condition that this does not threaten the other

[28] For example, the *Relaxin Opposition* in Europe. See: Beyleveld and Brownsword (n 5) 196-202.
[29] For example, the European Patent Convention and the Directive on the Legal Protection of Biotechnological Inventions. See: ibid 199.
[30] This is closely related to the Justice theory of John Rawls.
[31] Beyleveld and Brownsword (n 5) 198-202. The 'dignity as constraint' argument suggests that it is 'implicated in much recent thinking about the limits to be placed on biomedicine, reflecting the belief that biomedical practice in the twenty-first century should be driven, not by the vagaries of individual choice, but by a shared vision of human dignity that reaches beyond individuals.' See: ibid 29.
[32] Ibid 202-205. The 'dignity as empowerment' argument claims that 'it is the intrinsic dignity of humans that acts as the foundation for human rights.' See: ibid 27.
[33] Ibid 202.

agent's generic rights. As the PGC is a right-based theory, there are no direct duties on the agent himself. Hence, it is considered that an agent should have property of their own bodies, including the tissue.[34] Here, the holder of generic rights is being considered as an agent.

Nevertheless, this is not to say that the PGC would agree that the benefits of science and technology should be best left governed by minimal regulation.[35] It has been argued by Beyleveld and Pattinson that, *ceteris paribus*, *some* potential benefits 'must be available to all or available to none.'[36] This is because, for the PGC, any criteria allocating benefits/ resources must recognise the equal status of all agents as right-holders since an agent must act in accordance with the generic rights of all agents. In this sense, moreover, it is noted that priority should be placed on the level of generic condition of agency according to the criterion of degrees of needfulness for action, rather than the number of agents. In the cases which equal status cannot be secured, the PGC cannot permit discrimination between agents, considering that all agents are fundamentally equal. Now, the key question is how to maintain an equal status?

According to Beyleveld and Pattinson, an equal status can only be achieved by:[37]

1. Universal access;
2. Universal denial; or
3. Completely random allocation.

---

[34] Ibid 204. For further discussions, see section 6.3.1.
[35] Cf. the Nozick-style libertarians, see: Robert Nozick, *Anarchy, State, and Utopia* (Blackwell 1974). Also, Adam D. Moore, 'Owning Genetic Information and Gene Enhancement Techniques: Why Privacy and Property May Undermine Social Control of the Human Genome' (2000) 14 Bioethics 97-119.
[36] Deryck Beyleveld and Shaun D. Pattinson, 'Individual Rights, Social Justice, and the Allocation Of Advances in Biotechnology' in Michael Boylan (ed), *Public Health Policy and Ethics* (Kluwer 2004) 59-72.
[37] Ibid 66.

In the third situation, what constitutes the equality is the opportunity to be accessed and to be denied. In this regard, for example, since *some* researches (e.g., those aiming at maximising bodily existence) cannot be available for all, it must be led to cautious reconsideration. Hence, there must be some *smart* regulatory methods for the government to adopt.[38] In this sense, the free model cannot be *totally* accepted by the PGC in a certain amount of cases.

Overall, to deal with the sharing of the right to enjoy the benefits from the progress of science and technology, as long as there is a justification, whether a procedural or substantive one, based on the PGC, the generic conditions of agency are not necessarily harmed. Therefore, what we should care about is not which market model can better fulfil the positive as well as the negative rights – particularly not in the case with an over-enthusiastic focus on the benefits of scientific and technological advances. Rather, the PGC focuses on (1) whether the agents are treated as capable of giving a valid informed consent, which leads us to consider the procedural/ prior justification; and (2) how to reconcile competing rights. They are also related to our next question on the relationships with other rights.

2. The relationships with other rights

The second issue deals with the fact that the right to enjoy the benefits from the progress of science and technology often conflicts with other fundamental rights and freedoms. This concern, indeed, has been regularly addressed by several international norms. It has been pointed out, for example, by the UNESCO that:[39]

1. Technological Progress in the Interest of Peace and for the Benefit of Mankind

[38] Cf.: Roger Brownsword, *Rights, Regulation, and the Technological Revolution* (OUP 2008).
[39] UNESCO (n 11) 5.

(GA Res. 3384 (XXX)), adopted in 1975, noted that "while scientific and technological developments provide ever increasing opportunities to better the conditions of life of peoples and nations, in a number of instances they can give rise to social problems, as well as threaten the human rights and fundamental freedoms of the individual."

2. The World Conference on Human Rights (1993) reaffirmed the right to benefit from scientific progress (Paragraph 11 of the Vienna Declaration). The World Conference noted that certain advances, notably in *biomedical and life sciences* as well as in *information technology*, may have potentially adverse consequences for the integrity, dignity and human rights of the individual, and called for international cooperation to ensure that human rights and dignity are fully respected in this area of universal concern.
3. Serious challenges in relation to REBSP (the right to enjoy the benefits from the progress of science and technology and its applications) arise in connection with *bioethics and biotechnology*. The Universal Declaration on the Human Genome and Human Rights (1997), the International Declaration on Human Genetic Data (2003) and the Universal Declaration on Bioethics and Human Rights (2005), adopted by UNESCO, were adopted in response to these challenges.

(Re-paragraphed and emphasis added)

As regards the legal regimes discussed in this thesis, in Europe, the Preamble to the European Charter of Fundamental Rights states that '…it is necessary to strengthen the protection of fundamental rights in the light of changes in society, social progress and scientific and technological developments by making those rights more visible in a Charter.' On the other hand, Article 10(2) of the Additional Articles of the (Formosan) Constitution states that '[e]nvironmental and ecological protection shall

be given equal consideration with economic and technological development.'

It should be borne in mind, however, that it is not the aim of this thesis to discuss all (potentially) competing rights with respect to such a right in general, but to the biometric and RFID technologies and the privacy and data protection concerns over them. Accordingly, it must be recalled that in the field of ICT, new technologies should not put the right to privacy and data protection interests at risk (Chapter 2). As we have seen in Chapter 4, moreover, the PGC provides the criterion of degrees of needfulness for action to deal with the question of reconciling the competing rights in conflict. To concentrate on the core issue addressed in this thesis, i.e. privacy and data protection concerns over biometric and RFID technologies, our next step is to evaluate the concepts of privacy and data protection on the PGC ground.

6.3 The Concepts of Privacy

6.3.1 Spatial Privacy

Under an empirical assessment through the legal regimes considered here, bodily integrity[40] including both *physical and psychological integrity*, arguably, can be considered as a basic need of agency to be a prerequisite of an ability to act at all, whatever the purpose being pursued.[41] This is because an agent (A) acts through A's body: as A's body is attached to A, then to violate the integrity of A's body can

[40] This thesis regards the body integrity as including both *physical and psychological integrity*. It seems that Beyleveld and Brownsword term the physical integrity as the bodily integrity and the psychological integrity as personal integrity. See: Beyleveld and Brownsword, *Human Dignity in Bioethics and Biolaw* (n 5) 177. It shall be noted that to consider body integrity as a basic need under the PGC is to presuppose that agents are necessarily physical embodied beings. However, this might not be true when applying the PGC to all species. Nevertheless, by empirically looking at the Formosan legal regime, the agent here concentrates only on individuals i.e. human beings. See: Deryck Beyleveld and Roger Brownsword, *Consent in the Law* (Hart Publishing 2007) 51-52.

[41] Alan Gewirth, *Reason and Morality* (University of Chicago Press 1978) 54.

generically affect A's capacity to act at all or act successfully.[42]

The PGC, thus, grants generic rights to bodily integrity. However, it does not necessarily follow that A must be granted the *control* over A's body and its integrity. It is still arguable that other agents (B) might need to use A's body when B needs to act through A's body. Nevertheless, to grant A's rights to body integrity without granting A to control A's body is not a sincere grantee. This is particularly true when: (1) there is harm to her physical integrity to a severe extent which results in A being unable to act at all or act successfully through A's own body; and (2) A's psychological integrity is harmed to an extent which leads A to have serious objections or hesitations against A's holding of generic rights, so as to act for any purpose.

However, this does not follow the recognition of control over *subsequent* uses of A's body. Nevertheless, it must be noted that the right to *physical integrity* is not the only right covered in order to 'give the source person control over the use of his or her body parts after their removal.'[43] *Psychological integrity* as well as other concepts of privacy should also be considered. In this regard, the *functional* aspect of the claim should be taken into account for the analysis of the right to bodily integrity in relation to the concept of the right to privacy, particularly when the research/ application is focusing on the *subsequent* uses of the body parts. The relevant subsequent uses of the body parts with respect to the technologies considered include: (1) the use of these body parts (e.g., biometric samples) after they are *separated* from the agents; (2) the use *after the death* of the agents; and (3) the use without, or sometimes even against A's consent (e.g., via RFID technology in a function creep way). A further question, therefore, must be asked: to what extent can this be controlled? Is this control over a

[42] See: Beyleveld and Brownsword, *Human Dignity in Bioethics and Biolaw* 186.
[43] Ibid 177.

subsequent use also recognised?

To be consistent with the above discussion which indicates that an agent acts through its body, I shall firstly outline Beyleveld and Brownsword's justification for property rights, i.e., *the 'rule-preclusionary' conception of property.*[44] They remark that[45]

> A right to exclusive use of an object is necessary and sufficient to characterize property rights substantively, and that the essential function of a justification on the basis of a property right is to justify a right to exclusive use in a characteristic way.

Why should A be given such a level of control over its body then? This is because:[46]

(1) A's reliance on A's body is so strong that the challenge of the control over A's body itself places A's agency under threat; and
(2) Lacking control over A's body may cause specific generic harm to A, particularly in the cases that A's 'legitimate beliefs' over A's right to privacy have been interfered with, leading A to hold strong objections against uses impinging on A's right to body integrity. The 'legitimate beliefs' here 'makes persons particularly prone to attach religious and other deep, sometimes idiosyncratic, emotional significance to their bodies and body parts.'

It is pointed out, furthermore, that the second reason is especially crucial when A is unable to act through A's body, in particular when A cannot practically show A's

[44] Ibid 171-194. Also, Deryck Beyleveld and Roger Brownsword, 'My Body, My Body Parts, My Property?' (2000) 8 Health Care Analysis 87. For the applications of the 'rule-preclusionary' conception of property, see, for example: Shaun D. Pattinson, 'Directed Donation and Ownership of Human Organs' (2011) 31 Legal Studies 392-410.
[45] Beyleveld and Brownsword, *Human Dignity in Bioethics and Biolaw* 177.
[46] Ibid 187-188. For general arguments to justify why agents own their bodies in the rule-preclusionary sense, the two scholars offer three arguments. See: ibid 179-186.

consent, e.g., the control over A's removed body parts and A's body and body parts after death or when A is unconscious.[47]

On the basis of this conception, A owns A's body according to A's prima facie right, and such a right enables A to: (1) use A's body in any legitimate way (based on the PGC grounds); and (2) exclude B from using A's body. This is because A stands in a *particular relation*[48] to A's body that precludes A from depending on a case-by-case basis for A's right to use A's body and to exclude B from using A's body. In this regard, the biometric samples would imply exclusive use, subject to the waiver (with valid consent) or the overriding rights of others, whether individually or collectively, without articulating the specific right in every particular use. Such a claim does not mean, however, that the right to bodily integrity is an absolute right. Rather, it only holds a prima facie right to do what A wishes to do with A's body (as a positive right) or a prima facie right to prevent B doing what B wishes to do with A's body (as a negative right).[49] Furthermore, under the PGC, this claim only permits B to use A's body where B has A's consent or a right that outweighs A's right based on the criterion of degrees of needfulness for action.

It might be argued that, however, as it is not necessary for A to act through any of A's body parts (such as A's hairs, nails and so on), the argument of granting control over those 'attached parts that are not only renewable but can be removed without significant lasting harm on bodily integrity' may be not necessarily apply.[50] Nevertheless, the second reason provided above is able to reply to this objection:

[47] Ibid 188.
[48] Whilst A's body belongs to and metaphysically related to A, it functionally means that it is so related to A that A does not have to say why A should be able to use it or why A may exclude others from using A's body. See: ibid 188.
[49] See also: Pattinson, 'Directed Donation and Ownership of Human Organs' 396.
[50] Beyleveld and Brownsword, *Human Dignity in Bioethics and Biolaw* 188.

since they are closely related to A's 'legitimate beliefs' to the extent that A stands in a particular relation to them, to cause generic harm over those body parts is to be avoided under the PGC. This is of central importance to explain why the biometric samples and files are considered to be sensitive under the data protection regime. Specifically, to interfere with the control over such body parts may cause particular generic harm in relation to A's bodily integrity.[51]

A further issue, moreover, rests on the question of why personal (biometric) data and subsequent information can be 'owned' and related to an idea/ concept of property right applying the 'rule-preclusionary' conception of property. Indeed, this is not a new question. In Moore's article, on the basis of a Lockean model of intangible property,[52] he argues that[53]

> Intangible property of this sort can be owned – that the proper subjects of intangible property claims include medical records, genetic profiles, and gene enhancement techniques. Coupled with a right to privacy these intangible property rights allow individuals a zone of control that will, in most cases, justifiably exclude governmental or societal invasions into private domains.

Two sub-arguments have been justified in this article. First, personal data (information), as a type of intangible property, can be owned according to the 'no harm, no foul' principle.[54] Secondly, the author contends a 'fairly strong presumption in favour of individual privacy.'[55]

We shall have a little more to say in relation to consent issues. There are also

[51] Such harm to privacy usually overlaps other concepts of privacy, e.g., informational privacy.
[52] Moore (n 35) 98-103.
[53] Ibid 98.
[54] Ibid 101.
[55] Ibid 109.

further considerations in relation to the applications and guidelines on biometric samples and data, e.g., the legitimacy of transferring such samples and their subsequent uses. This will also be discussed in the next chapter.

With regards to the *right of not being spied on* or *the right to be let alone* regarding the restricted access of A and A's private space, regardless of whether the agent is aware of it or not, if an agent is being seriously spied on or disturbed to the extent that A's psychological wellbeing has been affected, there is a basic harm to A. This is particularly the case when the powerful prying eye comes from State authorities or private entities with special powers. This can also happen in the situations of function creep of RFID applications and the abuses of data filing, particularly for biometric data. The violation of such a right, in specific cases, can affect one's bodily integrity to the extent of fearing, worrying, and feeling ashamed to one's private beliefs to act successfully. This causes harm to a non-subtractive need.

With respect to *the protection of the living space and environment*,[56] it is argued by Gewirth that the need for shelter can be considered as a basic need. In addition, it has been addressed by Mills that 'even in societies that have no private property ownership rights, control of physical space is protected.'[57] To interfere with the *control* of the residential or any shelter space could therefore amount to a violation of generic needs.

It has been argued by the (German) government in *Von Hannover v. Germany*[58] that there is a *criterion of spatial isolation* in relation to the private space when deciding on a violation to the right to private life. Such a criterion appreciates the

[56] See also, section 4.3.2.
[57] Jon L. Mills, *Privacy: the Lost Right* (OUP 2008) 20. In his book the author exemplifies the North Korea as the discussing legal regime.
[58] *Von Hannover v. Germany* (App no 59320/00) (2004) ECHR 294, para 54.

place where the interference occurs when deciding whether there is a violation of the right to private life. It is limited to the situation in which an agent is in a secluded place out of the public eye where 'persons *retire* "with the objectively recognisable aim of being alone and where, confident of being alone, they behave in a manner in which they would not behave in public".'[59] However, this criterion to judge whether a place is under the 'public eye' has been considered as 'too vague and difficult for the person concerned to determine in advance' by the ECtHR.[60]

Two points shall be made in relation to the German *criterion of spatial isolation*. First, it is observed by Harris et al. that the objection against such a criterion rests on the reason that an agent 'must be able to a substantial degree to keep to himself what he is and what he does, if he wishes to do so.'[61] This observation is in line with the PGC reasoning, which requires that each agent must be equally treated as a holder of generic rights and must also reciprocally respect these rights in all other agents. Such rights shall be substantively respected *wherever* the agent is, for whatever purposes the agent acts, if the agent so wishes. The criterion thus fails to take into account the genuine means to keep the agent's generic rights.

Secondly, an agent can always waive benefits that the exercise of these rights affords her through valid consent as long as it is not causing any harm to others, or the harm can be justified. However, it does not necessarily follow that an agent always means to waive her benefits of the right to privacy whenever she is in a public place. This is closely related to the issues of reasonable expectations. Indeed, practice can frequently and inevitably reduce the scope of the right by affecting the expectations.[62]

[59] Ibid, para 54.
[60] Ibid, para 75.
[61] David Harris and others, *Harris, O'Boyle & Warbrick: Law of the European Convention on Human Rights* (2nd edn, OUP 2009) 368.
[62] Roger Brownsword, 'Informed Consent in the Information Society' (Durham CELLS Lecture,

In the case at hand, however, her clear appearance of her free will should be able to present her unwillingness of waiving the benefits of her right to privacy.

Nevertheless, it must be noted that in special cases, the rights of other agents may require the agents in question to be overridden according to the criterion of degrees of needfulness for action. Considering the case in J. Y. Interpretation No. 535, for instance, an on-the-spot police check involves police powers performing checks or street checks to enforce the law, interrogating persons, and executing other duties in public or private spaces can interfere with A's body integrity. In such a situation, because Article 2 of the Police Act sets out that the duties of the police are to *maintain public order* according to the law, to protect *social security*, to prevent any harm, and to promote people's welfare, A will not be permitted to reject the police power. This does not follow that, however, A's body integrity as well as A's privacy are no longer generic rights. It only means that A's integrity and privacy are overridden by the other generic rights according to the criterion of degrees of needfulness for action.[63] Furthermore, this overriding right (public interests) is far from absolute: it has to be further justified under the PGC reasoning. With this in mind, it is aptly required by the Honourable Justices that 'the requirements and procedures of police checks as well as legal remedies for unlawful checks must be prescribed clearly by the law.'[64]

6.3.2 Decisional Privacy

It has been noted that the right to develop personality, identity, or any deep emotional significance linked to an agent's bodily integrity is within the scope of the right to

Durham, 8 May 2012).
[63] See also: Beyleveld and Brownsword, *Human Dignity in Bioethics and Biolaw* 172.
[64] Paragraph 2 of the reasoning of J. Y. Interpretation No. 535.

privacy. Moreover, this group of rights also includes the establishment, development and termination of relationships with other agents and the outside world.[65] The autonomous character of decisional privacy thus will be emphasised when evaluating rights subject to this dimension and surrounding cases.

It is important to point out that, under the Gewirthian reasoning, individuals must 'be permitted to do anything they like, provided only that this does not directly or indirectly threaten the generic rights of others.'[66] Therefore, to deny A's decisional privacy by acting against A's free and voluntarily choice, either in those decisions concerning only A's own business, or establishing or changing relationships with others, is not to offer adequate protection to A's generic rights.

However, as previously mentioned, it does not follow that decisional privacy, along with other (non-absolute) generic rights, must always be permitted – it should not be permitted if it is conflicted with and prevailed over. In this respect, the Formosan landmark case of J. Y. Interpretation No. 554 provides an interesting example.[67] Two interests of decisional privacy are considered, namely *the right to maintain relationships with other human beings* and *the right to freedom of sexual activity*. As regards the former right, the marital relationship is at stake. According to the constitutional interpretation,[68]

> [m]arriage means a living agreement where a husband and a wife mutually engage with each other to live their lives together so that both may realize and develop their *respective* personalities. (emphasis added)

[65] See: Section 4.3.2.
[66] Beyleveld and Brownsword, *Human Dignity in Bioethics and Biolaw* 194.
[67] See: Section 5.4.2.
[68] J. Y. Interpretation No. 554.

The Court, here, implies that although a new relationship is established, decisional privacy of two agents should still be taken into account *independently*. Moreover, the Court accepts that 'every person is free to decide whether or not and with whom to have sexual affairs.' This covers the right to freedom of sexual activity. In the current case, these two rights conflict: to have sex with others might affect, usually in a negative way, the relationship between the two partners.[69]

In Dworkin's contribution he criticises that Himmelfarb[70] misunderstands John Stuart Mill's *On Liberty* as she confuses 'liberty as license', which means 'the degree to which a person is free from social or legal constraint to do what he might wish to do,' with 'liberty as independence', i.e., 'the status of a person as independent and equal rather than subservient.'[71] In this regard, according to the definition given by Anita Allen, decisional privacy, as freedom from any external influences on an individual's decision-making in relation to private affairs, might be misunderstood as what Dworkin terms 'liberty as licence.'[72]

Under the PGC, the concept of decisional privacy does not fit with the idea of 'liberty as license', which suggests that the value/ function of decisional privacy is a

[69] Different communities may have different rule-sets to operate in relation to such a particular type of consent. Beyleveld and Brownsword, *Consent in the Law* 340. Also, the Constitutional Court holds in paragraph 3 of the reasoning of J. Y. Interpretation No. 554 that 'as regards the type of restriction, if any, that must be imposed on sexual affairs between a married person and a third party during the subsistence of a marriage and whether or not an act in violation of such restriction should be made punishable as a crime, the problems must be dealt with by the norms of conduct to be determined by the legislature by taking into consideration how marriages and the family system should be protected *in light of the customs of the country, which vary from nation to nation*.' (emphasis added) In Taiwan, it seems that the value of marriage can override the interest of freedom of sexual activity *when conflicts happen*. However, under some circumstances, these two values may not necessarily be in conflict with each other. See: Paragraph 3 of the reasoning of J. Y. Interpretation No. 554.

[70] Gertrude Himmelfarb, *On Liberty and Liberalism: The Case of John Stuart Mill* (Alfred A. Knopf 1974).

[71] Ronald Dworkin, *Taking Rights Seriosly* (New impression with a reply to critics, Duckworth 2005) 262.

[72] Ibid 262-264. For a Taiwanese local discussion, see: Wen-Tsong Chiou, 'Comments on the Framework Problems of the Draft of Computer-Processed Personal Data Protection Law from the Perspective of the Conceptual Distinction between Information Self-determination and Information Privacy' (2009) 168 The Taiwan Law Review 176.

license that allows the external (such as social or governmental) constraint off. To view decisional privacy as 'liberty as license' is simply wrong because it is by virtue of vulnerable (in the sense of a vulnerable decision-making/ autonomy) agency that the generic rights are to be granted, and it imposes duties on other agent to respect the generic rights of the right-holder, rather than a protection from the external constraint.

It should be recalled that, on the basis of the dialectally necessity argument, 'I am required to claim that I am an agent is *sufficient* for me to claim that I have the generic rights.' However, this claim can only be applied to vulnerable agents instead of 'non-vulnerable agents.'[73] Whatever purposes chosen by the agent, these should always be able to motivate them to pursue the ends valued. Hence, as Beyleveld and Brownsword put:[74]

> [t]he most fundamental of these generic needs are the vary capacity to reason and make choices, life itself, and mental equilibrium sufficient to *translate a wish for something into activity designed to obtain what it is wished for*. (emphasis added)

With this in mind, the concept of decisional privacy under the PGC is *closer* to Dworkin's idea of 'liberty as independence'. More specifically, decisional privacy e.g., the capacity of an agent to decide her own identity, offers an intrinsically flexible capacity to an agent. This makes an agent able to voluntarily act for *whatever* purposes the agent has chosen.

Moreover, Dworkin defines 'liberty as independence' as a discriminate concept which distinguishes between forms of behaviour. Dworkin further suggests that when an agent places a high value on liberty as independence, he 'is not necessarily

[73] Beyleveld and Brownsword, *Human Dignity in Bioethics and Biolaw* 115.
[74] Ibid 115.

denigrating values or amenity, or even in a relative way.'[75] For example, if an agent exercises her right to decisional privacy, she does not automatically exercise this in favour of 'greater licence' when other values are not in a conflict. Dworkin's account of justice in 'liberty as independence' runs parallel to the Gewirthian account: the PGC requires empirical knowledge 'what concrete things instantiate generic rights, and also about the quantitative needfulness of various generic needs.'[76] Therefore, the PGC would not require attempts to suggest a clear list of the abstract categories (i.e., basic needs, non-subtractive needs, and additive needs) regarding which the PGC is couched.

Accordingly, to avoid a generic harm to agency, the collection and processing of biometric data and the employment of RFID technology should be taken into account in a 'liberty as independence' perspective. The use of such technologies should not be seen as freeing an agent from social or legal constraints. Rather, we should regard an agent as an end who independently and voluntarily acts for whatever purposes. In this regard, we should pay more attention to regulations in relation to the *profiling* of collection and processing of personal data. This is because such profiling results in affecting, or even re-shaping, an agent's bodily integrity according to the data controller's will, rather than the 'independent' will of the agent itself.[77]

We have seen that the interference with an agent's decisional privacy commits a violation of the PGC. However, there is no violation of the PGC if the agent has waived the benefit of the right to decisional privacy (as well as other generic rights) and it does not threaten the generic right of others.[78]

---

[75] Dworkin (n 71) 263.
[76] Beyleveld and Brownsword, *Human Dignity in Bioethics and Biolaw* 71.
[77] Chiou (n 72)177-180.
[78] Cf. the harm principle remarked by John Stuart Mill that 'the liberty of the individual must be thus

6.3.3 Informational Privacy

1. The 'nothing to hide' argument

The right to decide whether or not to disclose information emphasises what others (B) should *know* about the agent (A). A rather common objection against such a right can be termed the 'nothing to hide' argument, i.e., 'if A has got nothing to hide, A has nothing to fear/ lose'.[79] This argument is not unfamiliar, particularly for many governments with respect to their sweeping surveillance policies. For example, it was stated that 'if you've got nothing to hide, you've got nothing to fear' in the British government's campaign slogan for the citywide CCTV surveillance programme.[80] In Taiwan, the Confucian thinking of 'the Gentleman is magnanimous and has nothing to hide' and 'the petty man is always full of worries' has also been taken as a powerful reasoning of counterarguments. Indeed this argument is exactly the one that generally minimalises the privacy interest.[81]

In the light of this argument, it has been observed by Solove that, with the exception of some extreme yet unsuccessful forms, a general manner of such an argument can be recast as 'positing that all law-binding citizens should have nothing to hide'; thus only those engaged illegal conduct should carry an interest in concealing their unlawful activities.[82] Hence, the concept of the 'nothing to hide'

---

far limited; he must not make himself a nuisance to other people.' John Stuart Mill, *On Liberty* (first published 1859, Batoche Books 2001) 52.

[79] Daniel J. Solove, '"I've Got Nothing to Hide" and Other Misunderstandings of Privacy' (2007) 44 San Diego Law Review745-772.

[80] Jeffrey Rosen, *The Naked Crowd: Reclaiming Security and Freedom in an Anxious Age* (Random House 2004) 36, quoted from Solove (n 79)748.

[81] Daniel J. Solove, *Nothing to Hide: the False Tradeoff between Privacy and Security* (Yale University Press 2011) 21.

[82] Solove, '"I've Got Nothing to Hide" and Other Misunderstandings of Privacy' 751.

argument can be briefly summarised as when it comes to accessing and retaining individuals' information, '**there is no privacy violation if a person has nothing sensitive, embarrassing or illegal to conceal**.'[83] A related argument asserted by Richard Posner argues that 'the economist sees a parallel to efforts of sellers to conceal defects in their products.'[84] Therefore, in his view, the law should not protect '*the right to conceal discreditable disadvantage*'[85] under the concept of privacy.

The counter-arguments against these points are also common. The most popular one – I merely don't want to disclose *all* of my personal information to others, however, is not quite convincing. Indeed, the data controllers need not necessarily collect and process all kinds of personal data,[86] particularly irrelevant ones. Nevertheless, the 'nothing to hide' argument implies further criticisms to the protection of privacy. For example, during the 'periods of crisis' during which other rights and interests compete with privacy, national security interests should *always* outweigh privacy (and other individual rights).[87] Accordingly, for those 'essential' data collecting and processing circumstances, the nothing to hide argument remains a 'formidable' one.[88]

Solove himself replies that such an argument will face two counter-arguments. First, he identifies the problem of the argument that 'it myopically views privacy as a form of concealment or secrecy.'[89] This argument erroneously assumes that privacy is merely about hiding something wrong. However, by 'understanding privacy as a plurality of related problems,' it 'demonstrates that concealment of bad things is just

[83] Ibid 764.
[84] Richard A. Posner, *Economic Analysis of Law* (5th edn, Aspen Publishers 1998) 46.
[85] Ibid 46.
[86] Solove, *Nothing to Hide: the False Tradeoff between Privacy and Security* 23-24.
[87] Solove terms the argument the 'national security argument.' For further discussion, see: ibid 62-70.
[88] Ibid 24.
[89] Solove, '"I've Got Nothing to Hide" and Other Misunderstandings of Privacy' 764.

one among many problems caused by government programmes' when collecting and processing personal data.[90] Briefly, the concept of privacy is not *merely* about covering A's *bad things* from being known by B. Rather, this is about *the right to decide whether or not to disclose personal information*.

Secondly, he argues that the 'nothing to hide' argument is problematic even if there are *no bad things*, or even if there is *nothing* for A to hide. He addresses this as a Kafkaesque problem in connection with the 'nothing to hide' argument.[91] This conceptual of problem focuses on the issue of not being able to access one's personal data. He indicates problems in this respect: aggregation, exclusion, secondary use, and distortion.[92] He aptly argues that 'without greater transparency in data mining, it is hard to claim that programs like the National Security Administration data mining program will not reveal information people might want to hide, as *we don't know* precisely what is revealed,'[93] (emphasis added) Furthermore, he proceeds: 'having nothing to hide will not always dispel predictions of future activity.' This reasoning seems to be related to *the right to know and control how one's personal information will be used* and *the right to correct any inaccurate entries contained in one's personal information*.

What will the Gewirthian moral principles comment on this?

In the light of the first argument, from the perspective of A, A has a generic right to informational privacy, which is an prerequisite of an ability to act at all or with any general chances of success, *whatever purpose (E) is being pursued*. Therefore, regardless of the purpose, for example, no matter A wants to hide something sensitive

[90] Ibid 764.
[91] Solove, *Nothing to Hide: the False Tradeoff between Privacy and Security* 26-29.
[92] Ibid 27-28.
[93] Solove, '"I've Got Nothing to Hide" and Other Misunderstandings of Privacy' 766.

(E_1), to hide something embarrassing (E_2), to hide something illegal (E_3), or even to hide nothing (E_x), A has a generic right to informational privacy – if E is valuable to A. Indeed, I may even consider E to be even *morally* bad – what I need to attach is simply a positive value to my purpose on *non-moral* grounds, and to act according to these attached grounds to achieve the chosen purpose by my agency.[94] The 'nothing to hide' argument is simply wrong because it challenges the purpose of exercising a generic right.

Solove is, furthermore, correct in suggesting that the concealment of bad things cannot cover all aspects of privacy. However, this objection is by no means conclusive as the bad things, which may place an agent at risk, can still be the purpose of action without violating a right. Then, what if A's generic right causes risks or disadvantages to B (in the sense that Posner suggests, i.e., that the concealed discreditable disadvantage may violate other rights and interests)? From B's perspective, possessing correct information (on A) is necessary to be able to act for the vary possibility of acting; and to have additional information (on A) can improve B's capacities for successful action, regardless of B's purpose. Such information is thus either a non-subtractive or an additive need. The PGC places A under both negative and positive responsibilities to B. Such a positive obligation includes a number of informational obligations. For example, if A has HIV and fully acknowledges it, A is under a duty to disclose this to B before they are going to have any (unsafe) sexual intercourse, otherwise B will not be aware of the risk.

However, it must be noted that such a positive duty has its limits.[95] First, the PGC

[94] Gewirth, *Reason and Morality* 50-51, Deryck Beyleveld, *The Dialectical Necessity of Morality: An Analysis and Defence of Alan Gewirth's Argument to the Principle of Generic Consistency* (The University of Chicago Press 1991) 21-22.
[95] Beyleveld and Brownsword, *Consent in the Law* 175.

does not require agents to be superheroes; rather, the PGC requires them to be ordinary agents.[96] This can be termed the *comparable cost proviso*.[97] This is to say that A has positive duties only in a *proportionate* way (based on the measurement in terms of the criterion of degrees of needfulness for action) that do not bear incommensurate cost to A's own generic conditions of agency. Therefore, for example, if A has HIV and fully acknowledges it, the PGC does not require A to sacrifice A's informational privacy, *disproportionately* by publicly announcing or broadcasting it via the media. Secondly, neither does the PGC encourages B to take advantage of A's good will. If B is able to deal with B's generic requirements by B's own efforts, A's positive duties are simply not called into play. This is termed as the *own unaided effort proviso*.[98]

In J.Y. Interpretation No. 293 regarding *the right to personal financial informational privacy*, for example, no matter why A wants to hide A's personal financial information, A has a generic right to informational privacy. When A has a positive duty which suffers the cost of giving up A's informational privacy by disclosing A's personal financial information, so as to deal with state-owned banks' non-performing loans, the PGC does not require A to disproportionately disclose A's personal data.

Furthermore, the 'nothing to hide' argument fails to take the right to access one's personal information, including *the right to know and control how their personal information will be used, and the right to correct any inaccurate entries contained in*

[96] This is because the prevention or removal of transactional inconsistency should take priority over other criteria for resolving conflicts of duties since the former is the most direct way to fulfil the central requirement of the PGC. See: Gewirth, *Reason and Morality* 344-345. Also, Gewirth, *The Community of Rights* 47.
[97] Beyleveld and Pattinson, 'Individual Rights, Social Justice, and the Allocation Of Advances in Biotechnology' (n 36) 61.
[98] Ibid 61.

their information into account. As Solove points out, it 'assumes a particular view about what privacy entails to the exclusion of other perspectives.'[99] It should be noted that such rights do not only fall within the scope of the right to privacy, but may be necessary means to help realising other generic rights. For example, not being able to correct inaccurate personal health information may cause harm to health or life. Ignoring such rights thus should be avoided on the PGC basis since the agent should be granted necessary means to achieve the protection of generic rights.

Lastly, it must be noted that even if there is a conflict, A still has the *right to decide whether or not to disclose information, the right to know and control how their personal information will be used, and the right to correct any inaccurate entries contained in their information* – regardless of whether those rights are overridden by countervailing rights and interests or not. Therefore, there is in fact a privacy violation even if an agent is in possession of something sensitive, embarrassing or illegal to conceal – though this violation may be *justified* either in a procedural or substantive way.

2. Informational Privacy and Technology

Having mapped out the right to informational privacy, it is crucial to note that this is a right profoundly affected by modern technologies. It has been observed, for example, that '[i]nformation privacy is a fluid concept because its public recognition has coincided with the rise of modern technologies.'[100] It follows that a key task in the informational privacy regime is to make it absolutely clear as to how to deal with the changing concepts of informational privacy.

[99] Solove, *Nothing to Hide: the False Tradeoff between Privacy and Security* 29.
[100] Ming-Li Wang, 'Information Privacy in a Network Society: Decision Making Amidst Constant Change' (2010) 5 National Taiwan University Law Review 140.

The development of technology could affect the right to informational privacy in three different scenarios: (1) an agent (A) does not know that A's information has been collected, processed or disclosed; (2) the other agents (B, data controllers, e.g., the government) collect, disclose or process A's information against A's will; and (3) A waives A's benefits of the right to informational privacy.

First, in the case that A does not *know* that A's information has been processed, A is unable to control what B can know about him. Function creeps of certain information technologies such as *insensible* data mining via the RFID technology,[101] for example, can at least diminish the successful possibilities of A or to the extent leading A not being able to act at all, as A acts on the basis of the false assumptions. This type of violation against the PGC is equivalent to denying A's GCA.

Secondly, new technologies may be used as a medium to disclose A's information against A's will. This violates A's generic right. This frequently happens when B misapplies the 'nothing to hide' argument discussed above and disproportionately extends A's duties to B. For example, conditioning the issuance of an ID card upon comprehensive compulsory fingerprinting without (proper) purpose (as the factor in J. Y. Interpretation No. 603) is to violate A's *right to decide whether or not to disclose information*. This scenario also includes the prevention of potential objections. The system without the opt-out clause for reading out sensitive biometric information on RFID tags is an obvious example in such a scenario.

As regards the third scenario, the substantial changes of cutting-edge information and communication technologies provide motivations to agents to disclose/ share information with others. For example, a legal professional may want to post her

[101] For example, consumer information can be read while a tag attached on an agent who walks in a mall/ high streets with any warning signs reminding the agent about the RFID readouts.

contributions on the Social Science Research Network (SSRN)[102] so as to let more people acknowledge or even discuss/ follow her brilliant ideas, and a politician may be willing to post everything about her on her blog so as to conduct vigorous propaganda. In this trend it is reasonable to anticipate that A may tend to trade A's information 'given the right *price*.'[103]

However, this might lead to a presumption of the interest-based reasoning – after all, it seems correct to argue that '[g]iving away some personal data is not only acceptable, but also *desirable under the right conditions*.'[104] Nevertheless, to explore this issue more in depth, the fact that some netizens who would like to disclose their information for reasons other than 'exchanging' something for a corresponding price, or even for reasons that may have them hurt (such as disclosing the information that she will get drunk easily by drinking some specific types of wine, on her Facebook, might let others try to take advantage of her), shows that the *will conception* is to be applied to the right to informational privacy.[105] The latter is crucial in the revolutionary age of web 2.0[106] of information technology. This preference is not forbidden by the PGC. This is because there are no direct duties towards oneself under the PGC – the benefits of the generic rights can always be *freely* waived – provided that this waiving does not threaten the generic rights of others.[107] Nevertheless, there is no denying that there can be good, and essential, reasons to interfere with such voluntarily waives of the benefits of the right to informational

[102] http://www.ssrn.com/
[103] Wang (n 100) 143.
[104] Ibid 144. Cf. Richard A. Posner, 'The Right of Privacy' (1978) 12 Georgia Law Review 393-422.
[105] See also: Beyleveld and Brownsword, *Human Dignity in Bioethics and Biolaw* 81.
[106] Originally the unidirectional websites are produced for the web users (netizens) to view the content that was created by the website controllers. In contrast to these websites, the web 2.0 information technology allows users to communicate and collaborate with each other by using the web platforms as both the user and creators in the social media dialogue. Examples of web 2.0 include wikis (e.g., Wikipedia), blogs, video sharing sites (e.g., YouTube), social networking sites (e.g., Facebook and Twitter) and so on.
[107] Beyleveld and Brownsword, *Human Dignity in Bioethics and Biolaw* 194.

privacy, which are grounded in the protection of rights of a higher degree of needfulness of generic condition of agency.[108]

6.4 Comments on Personal Data Protection Provisions

6.4.1 Consent in the Data Protection Principles: the Procedure Justification

This subsection aims to offer a critical analysis of consent in the two data protection law regimes at hand. This will primarily draw upon Beyleveld and Brownsword's contribution: *Consent in the Law*. The work which operates with the PGC,[109] should be capable of maintaining the coherence of this thesis. This is crucial in relation to previous sections in which the will conception of rights has been analysed. This part will, moreover, include examples by reference to two data protection regimes. We shall be able to identify and respond to the problems that arise out of these examples.

To begin, it should be noted that it is not the intention of the thesis (as well as any PGC-based work) to overestimate or undervalue the role of consent. This is because this mistake falls into the misunderstanding of thinking that 'consent is the necessary justifying reason (the Fallacy of Necessity),' while the latter commits the error of thinking that 'consent is a sufficient justifying reason (the Fallacy of Sufficiency).'[110] Indeed, such fallacies have been noted by theWP29 in its *Opinion on the Definition of Consent*:[111]

[108] Ibid 81.
[109] Beyleveld and Brownsword, *Consent in the Law* 32.
[110] Ibid 355. Also, Roger Brownsword, 'Consent in Data Protection Law: Privacy, Fair Processing and Confidentiality' in Serge Gutwirth and others (eds), *Reinventing Data Protection?* (Springer 2009) 90-92; Roger Brownsword, 'The Cult of Consent: Fixation and Fallacy' (2004) 15 King's Law Journal 223.
[111] Article 29 Data Protection Working Party, *Opinion 15/2011 on the Definition of Consent* (01197/11/EN, WP187, 2011) 2, 7.

> Consent is *one* of several legal grounds to process personal data. It has an important role, but *this does not exclude* the possibility, depending on the context, of other legal grounds perhaps being more appropriate from both the controller's and from the data subject's perspective.
>
> The order in which the legal grounds are cited under Article 7 is relevant, but it *does not mean that consent is always the most appropriate ground* to legitimise the processing of personal data. (emphasis added)

In this case, it should be emphasised that both procedural, i.e., consent, and substantive justifications are allowed under the PGC; it is 'the right kind of justification has to be applied in the right kind of way' that should be taken into consideration.[112] Therefore, the use of consent in the correct context is crucial. As the WP29 puts, if consent is not rightly applied in practice, 'this would *weaken* the position of data subjects.'[113] (original emphasis)

To avoid the Fallacy of Necessity, i.e., the worship of consent, it must be noted that consent, as a procedural justification, depends on the engagement of the main claim (either a right or a duty).[114] In other words, since 'what determines whether such acts are morally permissible is not the presence or absence of consent but the application of background duties (or rights),'[115] it should bear in mind that 'if there is no right there is no claim' and 'no right, with or without consent, adds up to no claim.'[116] Hence, consent should not be considered in a free-standing way. In this

[112] Beyleveld and Brownsword, *Consent in the Law* 337.
[113] Article 29 Data Protection Working Party (n 111)10.
[114] Deryck Beyleveld and Shaun D. Pattinson, 'Moral Interests, Privacy, and Medical Research' in Michael Boylan (ed), *International Public Health Policy and Ethics* (Springer Netherlands 2008) 52.
[115] Brownsword, 'Consent in Data Protection Law: Privacy, Fair Processing and Confidentiality' 91.
[116] Ibid 92. Also, Gavin Phillipson, 'Transforming Breach of Confidence? Towards a Common Law Right of Privacy under the Human Rights Act' (2003) 66 Mod L Rev 726.

regard, consent should be regarded as a safeguard[117] which is operated as a defence rather than a cause of action.[118]

Furthermore, under the PGC reasoning, a data subject's (G, who is also a consent-giver) consent should be the primary consideration according to the principle of the 'priority of consent,'[119] which demonstrates that wherever possible, the consent-receiver (R, normally the data controller or the third party) should always firstly seek G's consent 'rather than doing the wrong and then seeking to justify it by reference to overriding rights.'[120] This is because the existence of consent offers two benefits: (1) it provides R with a licence to do X, whatever X may be; and (2) R can act without 'having to engage contestable substantive justifications.'[121] Additionally, under the Formosan privacy framework focusing on the right of personality, consent must always be taken into account seriously in order to reflect the self-determination/ autonomy characteristic of such a right. In this regard, consent functions as opposing the wrongdoings.

There is, on the other hand, also a need to avoid the Fallacy of Sufficiency. The opinion of the WP29 identifies that consent is not the only ground for lawfulness.[122] It notes that although the other grounds in Article 7 of the Data Protection Directive require 'a "necessity" test, which strictly limits the context in which they can apply,' it does not follow that consent 'leaves more margin of manoeuvre than the other grounds.'[123] Moreover, it is noted that 'obtaining consent does not negate the

[117] Article 29 Data Protection Working Party (n 111) 7.
[118] Beyleveld and Brownsword, *Consent in the Law* 242.
[119] Ibid 337. The principle of 'priority of consent' can be understood by referencing Beyleveld and Brownsword that 'in the absence of consent, a wrong will be done to agents whose rights are violated even if, all things are considered, the wrongdoing can be substantively justified as the lesser of two evils.' Ibid 63.
[120] Ibid 62.
[121] Ibid 63.
[122] Article 29 Data Protection Working Party (n 111) 7-8.
[123] Ibid 7.

controller's obligations under Article 6 with regard to fairness, necessity and proportionality, as well as data quality,' and 'nor does obtaining consent allow the circumvention of other provisions, such as Article 8(5).'[124] However, these reasons are not explicit enough to distinguish the functions and features of consent. The features of the consent thus require further explanation.

First, consent plays a role as the procedural, rather than substantive, justification of violations.[125] Such a procedural justification refers to an authorising act or decision rather than justifications referring to 'some set of background standards characterising (in the justificatory argument) particular acts as permitted (including required).'[126]

Secondly, consent can only be justified in an 'agent-relative' way.[127] Only the agent (G) who gives the consent is precluded from asserting that it has been wronged. Such a consent which precludes wrongdoing is not a general waiver to all benefits of all agents. Other agents can still claim their rights to which G has given its consent. For example, although G has consented to R to collect and process its personal data, it precludes G, and merely G, from denying or asserting anything to the contrary of G's given consent. Where there is any data involving any other agent, no matter whether G's data is related or not, R has to rely on other justifications.

Thirdly, by doing the authorised act (X), R does no wrong to G.[128] This has to be distinguished from the circumstances of violation which are justified by reference to overriding rights. As regards to the latter situation, there are some tests/ criteria to strike a balance between competing interests. This can surely result in the idea that

[124] Ibid 7.
[125] Beyleveld and Brownsword, *Consent in the Law* 61.
[126] Ibid 61.
[127] Ibid 61-62.
[128] Ibid 62.

consent leaves no more 'margin of manoeuvre than the other grounds'[129] since there are *different forms* of justification. Hence, to violate a right without consent is not necessary to act in a way that cannot be justified substantively.[130]

Accordingly, the function of consent as a procedural justification must not be confused with substantive justifications: the former authorises the action (X) for the consent receiver does to the giver, it follows that the former therefore does no wrong to the latter: the consent receiver's doing X to the giver is permissible.[131] For the substantive justifications, they are justified by referencing to 'overriding rights' or things considered as the lesser wrong.[132] For the sake of substantive justifications, e.g., public interests or other compelling rights and interests, doing X without consent might still be justified under the PGC, or any right-based theoretical framework.[133] Overall, the consent as 'procedure justification is one thing, substantive justification is quite another.'[134] It should be kept in mind that the validity of such substantive justifications by which G and R are bound rather than G's consent should appeal to the general principles of the PGC.[135]

With respect to the observations of the WP29 opinion, the obtaining of consent does not (1) negate the obligations of data controller; nor (2) allow the circumvention of other provisions. It should be noted that, moreover, in its opinion on the definition of consent, the WP29 also underlined that there are issues in relation to the conditions of *valid* consent and the operation of consent in the context of private or public wrong, e.g., the right of individuals to withdraw their consent; consent given before the

[129] Article 29 Data Protection Working Party (n 111) 7.
[130] Beyleveld and Brownsword, *Consent in the Law* 238-239.
[131] Brownsword, 'Consent in Data Protection Law: Privacy, Fair Processing and Confidentiality' 89.
[132] Ibid 89.
[133] See: ibid 96-97.
[134] Beyleveld and Brownsword, *Consent in the Law* 239.
[135] Ibid 336.

beginning of the processing; requirements regarding the quality and the accessibility of the information. Such an observation made by the opinion of the WP29, is able to show the recognition that 'the relevance of consent might reflect it significance by according it various degrees of justificatory weight.'[136] In the case of what the opinion means, arguably, it might be taken to indicate that the WP29 prefers a smaller role for consent.[137]

Having undertaken the groundwork, we are now able to identify and comment on the problems of Article 6 of the PDPL. Article 6(1) of the PDPL states:

> Personal information of medical treatment, genetic information, sexual life, health examination and criminal record should not be collected, processed or used. However, the following situations are not subject to the limits set in the preceding sentence:
>
> 1. when in accordance with law;
>
> 2. when it is necessary for the government agency to perform its duties or for the non- government agency to fulfil the legal obligation, and when there are proper security measures.
>
> 3. when the Party has disclosed such information by himself, or when the information concerned has been publicized legally;
>
> 4. when the personal information is collected, processed or used under certain methods by a government agency or an academic research institution based on the purpose of medical treatment, personal hygiene or crime prevention statistics and/or study.

[136] Ibid 231.
[137] Article 29 Data Protection Working Party (n 111) 7-8.

The confusion of the *integrity* of consent under the PDPL can be identified by comparing: (1) the absence of the consent justification when collecting and processing sensitive personal data (Article 6); with (2) the existence of such a procedure justification regarding non-special categories of personal data (Articles 15(II) and 19(V)). In this regard, it might lead to the misunderstanding that the more sensitive personal data is involved, the less consent from the data subjects is demanded.

The primary clarification should be the identification of, if at all, to what extent rights are covered by the law. Under Article 6, the relevant right is the protection of special categories of personal data. Given the sensitive character of such data, the law provides a higher standard of protection by forbidding the collection and processing of such data in general. Consequently, the higher protection of sensitive categories of personal data, which places autonomy at the heart of the data protection regime, would fit with the pattern of any will-based approach.

Arguably, since consent can reflect individual autonomy to some extent, it should be a root justification with respect to sensitive personal data. The function of consent here could signal concession with regard to the benefits covered by the right and assume a new set of rights and obligations.[138] This is particularly crucial in taking the *rule-preclusionary conception of property* into account: G should be granted a right to *control* G's body and G's body parts, including those body parts which have been removed or tissue containing genetic information about G, e.g., biometric data. What the WP29 states may reflect that 'the notion of consent is traditionally linked with the idea that the data subject should be in control of the use that is being made of his data.'[139] Hence, the idea that consent should play a more central role in relation to

[138] Beyleveld and Brownsword, *Consent in the Law* 238.
[139] Article 29 Data Protection Working Party (n 111) 8.

protection of sensitive personal data seems to be favourable. Accordingly, there must be something inadequate in relation to the integrity of consent in this provision.

However, to avoid committing mistakes, in particular the Fallacy of Necessity, there is a need to assess this claim in a more careful way. It should be, firstly, recalled that if there is no violation of R, there is no need to call for any form of justification.[140] Moreover, in the absence of consent, the violation of the rights entails that a wrong has been done.[141] Such a wrong can only be justified by a PGC-sensitive substantive justification.[142] Hence, to justify the violation, R will need to have a substantive justification provided by antecedent and overriding rights and interests.

Now, this Formosan provision, unlike Article 8(2)(a) of the Data Protection Directive, does not mention the justification regarding consent. However, nor does it prohibit the procedural consent as is referred by Article 8(2)(a) of the Data Protection Directive. Thus, at least in the private sector, according to the principle of the priority of consent, where practicable, R should firstly seek G's valid consent.

Moreover, considering the role and integrity of consent under Article 6, one has to consider whether the absence of a rule on consent is due to the misgiving that consent might interfere with legitimate public interests covered in the substantive justifications. In this regard, the first two exemptions of Article 6 concern the binding force of legislation and the third one is related to the principle of Estoppel. The forth exemption is more crucial with respect to the central issue of the thesis. We shall look at this in the next subsection.

[140] Beyleveld and Brownsword, *Consent in the Law* 238.
[141] Ibid 238.
[142] Ibid 238.

6.4.2 The Right to Academic Research and Its Benefits in the Data Protection Law Regime: the Substantive Justification

The starting point of this subsection is one of a few substantive justifications under Article 6 of the PDPL: a governmental or private academic research institution may collect and process sensitive personal data (including biometric data on the basis of the purpose of medical treatment, personal hygiene or crime prevention statistics and/or study). Critics argue that it is, however, problematic if this is done without the valid consent of the data subjects. This is because, as mentioned above, Article 6 itself does not clearly take consent as a justification and might invite the misleading interpretation that the research 'privilege' overrides the right to information self-determination.[143]

The PGC allows the possibility of the justification of the 'right-violations.'[144] Since the right to privacy is not an absolute right, one cannot immediately deny that there are chances for the research value to override the right to privacy as such. However, if the research value is capable of overriding the right to privacy and the right to protect personal data, 'then it must be conceived of as itself protecting fundamental rights and values.'[145] This is because only a right to generic condition of agency with more importance of needfulness for action can override the less important *right to generic condition of agency*. It can be argued that the research value may be considered as a generic condition of agency since it is at least an additive good to improve the data subject's purpose-achieving ability. Again, the critical point is whether such a 'public interest' is proportionately regulated and

[143] Ching-Yi Liu, 'Not So Improved: Initial Commentry on the Personal Data Protection Law' (2010) 183 The Taiwan Law Review153.
[144] Beyleveld and Brownsword, *Consent in the Law* 297.
[145] Deryck Beyleveld, 'Data Protection and Genetics: Medical Research and the Public Good' (2007) 18 King's Law Journal 276.

managed by effective safeguards, such as strict rules or anonymisation of data to be approved through the institutional framework when these competing rights and interests are *in conflict*.

The PDPL does not itself define the scope of the exemption and the other types of the 'public interest' with respect to the forth justification of the violation of Article 6. Instead, it asks the administrative authority (the Ministry of Justice)[146] to prescribe the content and scope of the public interest in the enforcement rules. This is permitted by the PGC since some acts are to be classified morally optional.[147] Though an act does not result in a private wrong through a *direct* application of the PGC, it may be justified by virtue of an *indirect* application of the PGC.[148] In the current case, the authority can be viewed as a competent decision-making governmental body applying the PGC – if the later regulations, which should assist in defining the shape and scope of *individual rights* and to 'preserve the context in which autonomous agents will enjoy the opportunity to flourish as members of a community committed to human rights and responsibilities,'[149] are in line with Gewirthian principles.

The rules set out by administrative authorities (quasi legislations) may not be *necessarily* followed by the courts. This is because, on the basis of the separation of power, the respect of the independence of the judicial powers and the quasi legislations are only taken into account by courts in reaching decisions.[150] Consequently, the Gewirthian principles should also be taken into account by the

[146] Article 6(II) states that: 'The rules of the range, procedure and any other items to be followed concerning Item 4 of the preceding Paragraph should be set by the government authority in charge of subject industry at the central government level in conjunction with the Ministry of Justice.'
[147] Examples can be found at: Beyleveld and Brownsword, *Consent in the Law* 289.
[148] Ibid 289.
[149] Ibid 271. It must be noted that this is only one of the general guidelines regarding the justification of the public wrong. A more detailed discussion with respect to such guidelines will be presented in the next Chapter.
[150] For relevant English legislation, see: Colin Turpin and Adam Tomkins, *British Government and the Constitution* (6th edn, CUP 2007) 473-478.

latter judicial review.

Turning to the debate in relation to the comparison between the right to informational self-determination, the right to privacy, and the right to benefit from advances in science and technology, indeed, there is no explicit provision emphasising that consent should be put in a central position in the Formosan data protection law regime.[151] However, it is noted that as long as the two interests can co-exist, a permissive approach should be maintained. Furthermore, when applying the Gewirthian reasoning to interpret the 'public interest', it must be borne in mind that the equation shall rest firmly on the generic conditions of agency. This shall not favour the opinion that a substantial serious harm to a particular agent is outweighed by the sum of individually negligible goods to the other agents within the collective sphere. Hence, the need for individual consent should not always give way to the 'public interest.'

Moreover, the central purpose of the PDPL is to govern the collection, processing and use of personal information *so as to prevent harm on personality rights*, and to facilitate the proper use of personal information. Since the principle of the priority of consent plays a central role under the PGC architecture to prevent generic harm on agents, the State should take the following criteria into account:[152]

1. Not to strict the exercise of the generic rights unless the agents concerned specifically consent to such a limitation (procedural justification) or for the sake of equivalent or overriding rights of other agents (substantive justification; and

[151] It should be noted that in the European law regime, the centrality of consent with respect to the collection and processing of sensitive personal data has been clearly emphasised by the ECHR. In other words, without explicit consent, the processing of sensitive data will engage Article 8.1 of the ECHR. See: *Z. v Finland* (1998) 25 EHRR 371. Also, Beyleveld, 'Data Protection and Genetics: Medical Research and the Public Good' 284. For a later comparison between the European and Formosan data protection law regimes, see Chapter 8 of the thesis.
[152] Beyleveld and Brownsword, *Consent in the Law* 290.

2. To consider necessary settlement for

    (1) Good community order (in a moral optional sense); and

    (2) The settlement of a genuine moral disagreement as to the permissibility of conduct.

However, as previously suggested, different values and interests do not always necessarily come into conflict. Under a broad conception of privacy, those 'medical research concerned with increasing life choices and improved quality of life,' and those crime-preventing researches concerned with securing personal space, can also be thought of as privacy values.[153] This invites the introduction of 'the co-operative model.'[154] We shall look at this in the following chapter.

6.5 Summary

Until now, this thesis has dealt with understanding the concept of privacy in both European and Formosan legal systems, by building on the general literature of regulations. This chapter has shown that modern technologies further complicate the concept of privacy and its regulation in both jurisdictions. Improving the availability of proper regulatory tools, then, needs to be considered. This shall be done by understanding whether particular technologies at issue present their own exceptional problems.

[153] Beyleveld and Pattinson, 'Moral Interests, Privacy, and Medical Research' 53.
[154] Deryck Beyleveld, 'Conceptualising Privacy in Relation to Medical Research Values' in Sheila AM McLean (ed), *First Do No Harm: Law, Ethics and Healthcare* (Ashgate Publishing 2006) 156-158 and Beyleveld, 'Data Protection and Genetics: Medical Research and the Public Good' 275-289.

Chapter 7

Implementing the PGC: Guidelines for Legal Regulations to Facilitate Dealing with Privacy and Data Protection Issues Regarding Technologies

7.1 Introduction

In previous sections we have seen that generic rights, such as the right to benefit from advances in science and technology and the right to privacy, are prone to coming into conflict. We have also seen how the PGC deal with this and the comments in relation to current normative frameworks. We now have a basis on which to consider how guidelines should be set in a regulatory and legal context according to which the PGC will be governed.

Implementation of generic rights requires respondents/ legislatures who can effectively secure them.[1] The current global framework consists of inaccurate and antiquated rules that lack appropriate guidelines to deal with biometrics and RFID specifically.[2] This calls for smart regulatory strategies and the clarification of the law. In this light, this chapter aims to offer a series of guidelines to deal with the advanced technologies at hand. It must, however, be noted that the chapter does not intend to provide a comprehensive regulatory policy and a statement of legal rules, nor does it cover exhaustively all aspects of governance.

[1] Alan Gewirth, *The Community of Rights* (The University of Chicago Press 1996) 56.
[2] Section 5.2.2.

The legal regimes, following the dialectically necessary argument, must accept the idea that the PGC is the supreme principle of all rules directed at action on pain of contradicting their legal validity. Moreover, the alternative contingent argument from the acceptance of human rights shows that, if the principle of instrumental reason is correct, any legal system recognises human rights and considers that every human agent should be treated equally must treat the PGC as a necessary criterion of legal validity. It is assumed, therefore, that all agents/ parties involved in the discussion comply with the Gewirthian principle of morality.

However, it is unrealistic for the development and application of the PGC to presume an ideal legal regime where supremely rational agents universally seek to uphold, or at least to attempt to apply, the PGC.[3] A more plausible/ pragmatic way of giving guidance on a PGC basis is to apply PGC-values, or at least apply values that are not forbidden by the PGC, 'in ignorance or denial of the PGC as the supreme principle of morality.'[4]

This chapter will firstly introduce a model to avoid conflicts between competing generic rights. This will allow for the full range of rights at hand to be achieved to a large extent. Secondly, to define the abstract concept of the PGC in such a way that it can be practically measured, the design of a regulatory framework reflecting the requirements of a democratic society (in a PGC-oriented sense) will be proposed to guide future deliberation and action.

[3] Shaun D. Pattinson, *Influencing Traits Before Birth* (Ashgate Publishing 2002) 169.
[4] Ibid 169. See also, Deryck Beyleveld, *The Dialectical Necessity of Morality: An Analysis and Defence of Alan Gewirth's Argument to the Principle of Generic Consistency* (The University of Chicago Press 1991) 149-150, and Phil Bielby, *Competence and Vulnerability in Biomedical Research* (Springer 2008) 87.

7.2 The Co-operative Model

7.2.1 Introducing the Co-operative Model

1. The Conflict model and the Acceptance of A Broad Concept of Privacy

I have addressed that when there are *conflicts*, the application of the PGC can reconcile various competing rights and interests by employing the criterion of degrees of needfulness for action and successful action. To strike a balance between competing rights and interests, on the other hand, the traditional position in relation to the proportionality test has been coined the 'weak proportionality test' by Vries et al., which indicates the consistence of

> a mere balancing of a fundamental right and another interest – for example: privacy and crime control – does in fact not offer any guarantee for the preservation of that fundamental right, since the approach itself assumes that preserving the one per definition implies weakening the other, and vice versa.[5]

This type of test excludes the possibility that both interests considered may be fostered and protected in an optimal way since it sees the balancing test as weighing one interest *against* the other.[6] For example, with respect to the relationship between data protection values, particularly privacy, and the right to benefit from advances in science and technology, this model suggests that the former interests always conflict with the latter one.[7] This has been termed the '**conflict model**.'[8] It views competing

[5] 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 2011) 21.
[6] Ibid 21.
[7] See for example: *R v Department of Health ex p. Source Informatics* [1999] 4 All ER 185, [2000] 1 All ER 786, cited from Deryck Beyleveld, 'Conceptualising Privacy in Relation to Medical Research Values' in Sheila AM McLean (ed), *First Do No Harm: Law, Ethics and Healthcare* (Ashgate Publishing 2006) 152.

rights as a zero-sum trade-off and holds that the right to privacy does not in any way, or at least not in a realistic fashion, support advances in science and technology. For example, Posner and Vermeule argue that '[a]t the security-liberty frontier, any increase in security requires a decrease in liberty.'[9] Such a model can be summarised as follows:

a. For those who consider that privacy values should always give way when there is a conflict, endorsing a *narrow conception of privacy*,[10]

   (i) The data subjects have a duty to participate in the application of such technologies by giving up their personal data, including very sensitive data such as biometric data. In this regard, valid consent is not required unless there is a higher right/ interest involved.

   (ii) The data subjects may lose their control over their personal data since the benefits of such applications prevail over privacy values. Any secondary/ further use with respect to personal data such as associating with the RFID system may be easily (or, abusively) justified.

   In this light, however, there is a risk that the value of consent is diminished to an extent that individual rights and human dignity are undervalued or even ignored. This contradicts the principle of the priority of consent.[11]

   Moreover, it is arguable that the participations in the research and application

[8] Beyleveld, 'Conceptualising Privacy in Relation to Medical Research Values' 155.
[9] Eric A. Posner and Adrian Vermeule, *Terror in the Balance: Security, Liberty and the Courts* (OUP 2007) 12.
[10] It is argued that, normally, the conflict model is associated with the narrow concept of privacy. Beyleveld, 'Conceptualising Privacy in Relation to Medical Research Values' 156.
[11] Section 6.4.1.

will necessarily result in benefits for science and technology. One must firstly justify whether there is a generic right to research (without leading to any specific interest) or a generic right to apply certain technology (as an end). Even if there are such generic rights, one has to, moreover, justify that they can *always* override the right to privacy.

On the basis of empirical research, it has been pointed out that the narrow conception of privacy and data protection results in a performance problem: 'there are black boxes and lacking mechanisms to ensure an effective data protection.'[12]

b. In contrast, for those who maintain that privacy values should always override benefits of science and technology, since the right to privacy is not an absolute right, there must still be chances of fallacy. In fact, even the most extreme privacy advocates rarely suggest that privacy values should always override the benefits of science and technology. Moreover, there is a tendency for supporters of a narrow conception of privacy to regard the right to privacy as a personal interest while seeing the right to benefit from advances of science and technology as a general public interest.[13] Under a Utilitarian calculus, which should be familiar to those who adopt of narrow conception of privacy, this situation comes into play frequently.

Mention should also be made to the fact that 'if there is a high concern of privacy, it is merely communicated. Mostly there is a low interest in

[12] Daniel Guagnin, Leon Hempl and Carla Ilten, 'Privacy Practices and the Claim for Accountability' in René von Schomberg (ed), *Towards Responsible Research and Innovation in the Information and Communication Technologies and Security Technologies Fields* (Publications Office of the European Union 2011) 103-104.
[13] Beyleveld, 'Conceptualising Privacy in Relation to Medical Research Values' 156.

enhancing privacy.'[14] Consequently, on the basis of the narrow conception of privacy, even though privacy concerns are highly valued, privacy may still not prevail.

However, it might be incorrect to always regard privacy/ data protection values and other values as belonging to two mutually exclusive sets. In other words, there might be/ is a possibility for data protection values, particularly the right to privacy, and the right to benefit from advances in science and technology of being capable of supporting each other. Indeed, there are counter-arguments to the conflict model of the balancing test. For example, the Privacy Advisory Committee for Scotland indicates that when justifying the processing and use of person data for medical research purposes, the explanation of public interest (in Article 8 of the ECHR) should refer to both 'the encouragement of good medical research and the protection of patient privacy.'[15] Furthermore, with respect to the relationship between national/ public security and privacy, Solove disagrees with the 'all-or-nothing argument' by arguing that the two interests need not be mutually exclusive.[16] Vries et al., moreover, by taking the 'necessary in a democratic state' test in relation to the ECtHR judgements, propose a 'stronger proportionality test,' which contends that there is a possibility to reconcile the multiple values.[17] This is because, they argue, the ECtHR criteria of balancing 'encompass[es] the possibility to refuse a measure because it harms the essence of a fundamental right or of the constitutional order, even if it can

[14] Guagnin, Hempl and Ilten (n 12) 103.
[15] Graeme Laurie and Nayha Sethi, 'Information Governance of Use of Patient Data in Medical Research in Scotland: Current and Future Scenarios' (*Scottish Health Informatics Programme (SHIP)*) <http://www.scot-ship.ac.uk/sites/default/files/Reports/Scoping_Report_Final_August_2010.pdf> accessed 6 August 2011, 8.
[16] Daniel J. Solove, *Nothing to Hide: the False Tradeoff between Privacy and Security* (Yale University Press 2011) 33-37.
[17] Vries and others (n 5) 21-22. Also, David Wright and others, 'Precaution and Privacy Impact Assessment as Modes towards Risk Governance' in René von Schomberg (ed), *Towards Responsible Research and Innovation in the Information and Communication Technologies and Security Technologies Fields* (Publications Office of the European Union 2011) 93-94.

be shown that this measure can effectively realise another legitimate interest.'[18] They suggest that, furthermore, there is an 'even stronger' proportionality test requiring to 'explore if there are alternative measures that allow for the realisation of the legitimate interest in a way that does not affect the fundamental rights in the same way as the proposed measure.'[19]

Nevertheless, there are two problems with respect to Vries and others' model, i.e. the stronger proportionality test. First, it is doubtful that the model remains a type of *balancing* test since there is no conflict between multiple values. Vries et al. state that, indeed, this issue is no longer a 'balance' between two values; instead, it is an answer to a series of questions in relation to the protection of fundamental rights and freedoms in democratic constitutional states.[20] Accordingly, instead of using the term 'weak proportionality test' and 'stronger proportionality test,' the proposed model builds upon the basis of what Beyleveld coins the 'conflict model' and the '**co-operative model**.'[21]

Secondly, the context of this idea and the justification of the argument have not yet been clearly spelt out in general terms. This deserves further attention. Briefly, the central idea of the co-operative model is that there is the possibility for two sets of values of being capable of supporting each other rather than coming into conflict. For example, with respect to the issues at stake:

a. The fulfilment of data protection requirements, particularly the protection of the right to privacy, can support applications of modern technologies. By

[18] Vries and others (n 5) 21-22.
[19] Ibid 22.
[20] Ibid 22. Also, Wright and others (n 17) 94.
[21] See: Beyleveld, 'Conceptualising Privacy in Relation to Medical Research Values' 156-158. Also, Deryck Beyleveld, 'Data Protection and Genetics: Medical Research and the Public Good' (2007) 18 King's Law Journal 275-289.

improving data subjects' trust, for example, not only the willingness of being subjects in a database, but also the chance of collecting more accurate and updated personal (sensitive) data will be expanded; and

b. Conversely, the applications of modern technologies may improve security and convenience of the private lives of individuals (including considerations of privacy values) as well as public interests. For example, the implementation of PETs[22] can prevent unnecessary or unwanted processing of personal data. The right to benefit from advances in science and technology can also provide individuals with more control over their private lives by providing them with more options. This fits with the concept of decisional privacy and informational privacy under the broad conception of privacy. Indeed, the co-operative model reflects the acceptance of broad conception of privacy, which is in line with the PGC.

We have considered that the conflict model is commonly associated with the narrow conception of privacy while the co-operative model tends to be associated with a broad conception of privacy. However, there remains a possibility for the conflict model to operate in relation to a broad conception of privacy. Nevertheless, such a relationship may generate a tension, or sometimes, a contradiction.[23] This is because under a European data protection model, to collect and process personal data for research and applications of science and technology, necessary rights protection measures must be taken into account. This is particularly crucial as Article 25 of the Data Protection Directive requires that transfer of personal data to a third country should only be allowed under the condition that the country in question ensures an

[22] Section 7.2.2.
[23] Cf: Beyleveld, 'Conceptualising Privacy in Relation to Medical Research Values' 156.

adequate level of protection. Specifically, according to Articles 4[24] and 25(1)[25] of the Data Protection Directive, a multi-national biometric database, which is more effective for achieving the purpose of protecting national and social security, whether transfer personal data within or outside the territory of the EU, must be handled according to respect for privacy. In this regard, the protection of privacy supports research and applications of science and technology. This is against the central idea of the conflict model that privacy interests always conflict with the benefits from scientific and technological advances.

2. The Justification of the Co-operative Model

Since the acceptance of a broad conception of privacy is a prerequisite of the co-operative model, the justification of accepting a broad conception of privacy will justify this model.[26] I shall thus provide support for a broad conceptualisation of privacy.

---

[24] Article 4 of the Data Protection Directive:
1. Each Member State shall apply the national provisions it adopts pursuant to this Directive to the processing of personal data where:
(a) the processing is carried out in the context of the activities of an establishment of the controller on the territory of the Member State; when the same controller is established on the territory of several Member States, he must take the necessary measures to ensure that each of these establishments complies with the obligations laid down by the national law applicable;
(b) the controller is not established on the Member State's territory, but in a place where its national law applies by virtue of international public law;
(c) the controller is not established on Community territory and, for purposes of processing personal data makes use of equipment, automated or otherwise, situated on the territory of the said Member State, unless such equipment is used only for purposes of transit through the territory of the Community.
2. In the circumstances referred to in paragraph 1(c), the controller must designate a representative established in the territory of that Member State, without prejudice to legal actions which could be initiated against the controller himself.

[25] Article 25(1) of the Data Protection Directive: The Member States shall provide that the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if, without prejudice to compliance with the national provisions adopted pursuant to the other provisions of this Directive, the third country in question ensures an adequate level of protection.

[26] Beyleveld, 'Conceptualising Privacy in Relation to Medical Research Values' 158.

The legal justification for the acceptance of a broad concept of privacy in the European human rights regime has been addressed in section 4.3 of the thesis. As regards the Formosan system, the adoption of the European data protection model together with a number of Constitutional Interpretations, e.g., J. Y. Interpretation Nos. 535, 585, 603 and 613,[27] can offer support to a broad concept of privacy. Hence, given the place of the ECHR in relation to EU law and the Formosan Constitution, it is legally justified to adopt the broad conception of privacy.

Apart from the legal aspects of justification, Beyleveld also suggests ethical reasons to justify the co-operative model. The first step is to relate the relationship between *privacy and benefits from advances in science and technology* to the relationship between *data subjects and data controllers*. In this regard, the rights and interests owned by data subjects cover both privacy and benefits from advanced science and technology since the European data protection model sets out the data protection law as a protection of fundamental rights and freedoms. On the other hand, from the controller's point of view, the data controller also possesses both interests. The two parties should, therefore, work in partnership since there is mutual respect for the rights of both parties.

Now, under the PGC thinking, in principle, data subjects must be treated as ends and possess negative and positive rights. In effect, data controllers must view those subjects 'not as information crops to be harvested for the common good or their own purposes, but as *partners* whose purposes are to be respected.'[28] In this light, the partnership between the two parties calls for the co-operative model, which asks the two parties to be treated equally, rather than competing with each other as suggested

[27] Section 5.3.2.
[28] Beyleveld, 'Conceptualising Privacy in Relation to Medical Research Values' 159.

in the conflict. This then presents a pragmatic reason justification of the co-operative model.

Indeed, to scrutinise the pragmatic reason in detail, we can consider game-theoretic ideas[29] to explain the behaviour of partners (data subject and data controller) in contexts where the outcome of actions depends on how agents chose to act in partnership games.[30] To do so, it is important for us to be sure how the situation is characterised. Here, I think of it as a prisoner's dilemma.[31] That is, 'the predicament of the parties in the ideal bargaining position is structurally equivalent to the situation' of the players of the game, which attempts to demonstrate '(1) that rational agents in a suitably idealized bargaining situation will agree on a specific, unique distribution of the benefits of cooperation, (2) what this distribution looks like, (3) that this distribution determines what is just, and (4), in case of Gauthier, that rational agents will comply with the terms of the bargain.'[32]

In the situation of the iterated prisoners' dilemma game, [33] it can be argued that

[29] According to Ross, Game Theory is 'is the study of the ways in which strategic interactions among economic agents produce outcomes with respect to the preferences (or utilities) of those agents, where the outcomes in question might have been intended by none of the agents.' For basic understandings on Game Theory, see: Don Ross, 'Game Theory' The Stanford Encyclopedia of Philosophy <http://plato.stanford.edu/entries/game-theory/> accessed 5 May 2012.

[30] Indeed, there might be other elements (e.g. data pirates) affecting the payoff of the game we are discussing. However, it is plausible for us to resist adding complications unless they are necessary. This is because we would not want the complications to 'obscure the basic forces at work.' As Baird et al. address, '[t]he test of a model is not whether it is "realistic," but whether it sheds light on the problem at hand.' Douglas Baird, Robert Gertner and Randal Picker, *Game Theory and the Law* (Harvard University Press 1994) 46.

[31] In the standard story of the pensioners' dilemma, there will be two accused persons. The police do not have enough information for a conviction. The police then separate the two men, and offer both the same deal in the interview: if neither of them confessed that the other guy is guilty, they will go to jail for a year. If they both betray each other, they will end up in jail for two years. But if one rat the other guy out and the other keep silent, then the one betrayed will go home free and the other will go to jail for five years. Each person must choose either to betray or remain silent; the decision of each is kept secret from the other. See, e.g., ibid 33.

[32] Bruno Verbeek, 'Game Theory and Ethics' The Stanford Encyclopedia of Philosophy <http://plato.stanford.edu/entries/game-ethics/> accessed 5 May 2012. See also, Steven Kuhn, 'Prisoner's Dilemma' The Stanford Encyclopedia of Philosophy <http://plato.stanford.edu/entries/prisoner-dilemma/> accessed 5 May 2012. For Gauthier's theory, see: David Gauthier, *Morals by Agreement* (OUP 1986).

[33] If two players play prisoners' dilemma more than once in succession and they act according to

without any cooperation (co-ordination), the agents involved in data collecting, processing and using are doomed to end up with the bad outcome even though there is a possible outcome that is better for game-players.[34] Hence, if agents are rational and thus put into place a rational plan of action, then acting according to the plan can be rational and beneficial 'even if so acting requires doing things that are not, considered from the standpoint of the moment of action, optimal.'[35] With this in mind, it is justified to believe that even if the mechanisms for the enhancement of the co-operative model may require agents to be less optimal and constrained (not pursuing their own best outcome), e.g., to increase preliminary investments and time, the model remains rational.

The better strategies for the (iterated) prisoners' dilemma have argued that players shall be nice, retaliating (i.e., not a blind trust), forgiving, and non-envious.[36] In his contribution Axelrod contends that,

> Its niceness prevents it from getting into unnecessary trouble. Its retaliation discourages the other side from persisting whenever defection is tried. Its forgiveness helps restore mutual co-operation. And its clarity makes it intelligible to the other player, thereby eliciting long-term co-operation.[37]

All of these are closely relating to the trust between rights holders. Indeed, through the way of satisfying each other by treating others as oneself, it is capable of enhancing incentives to cooperation. In this regard, to take cooperative actions against narrow self-interest can pragmatically generate better outcomes.

---

previous strategy of their opponent, the game is called iterated prisoners' dilemma.
[34] To put into economics jargon, the best outcome here is termed Pareto inefficient.
[35] Verbeek (n 32).
[36] Robert Axelrod, *The Evolution of Cooperation* (Basic Books 1984) 54.
[37] Ibid 54. For the counterclaims and justifications, see: Robert Axelrod, *The Complexity of Cooperation: Agent-Based Models of Competition and Collaboration* (Princeton University Press 1997).

However, it should be noted that the implication of game-theoretic ideas here is different from the utility/ moral contractarian (of Gauthier) theory. Both of the Gauthierian and Gewirthian theories claim that (human) agents must be treated with equal regard and respect.[38] However, rather than pursuing maximum happiness or Gauthier's discussion in the light of a co-operative bargaining position of constrained maximisation of self-interest, my intention of using game-theoretic analysis in relation to the pragmatic reasoning of the co-operative model is to minimise the risk of violating generic rights in so far as it is possible to do so. Accordingly, the full avoidance of generic harm is the highest-ranked outcome – although this is not always possible. In other words, there remains a possibility of conflict under the co-operative model. I will return to this point later.

I have provided support and justification for a broad conception of privacy. It is noted that the conflict model is normally coupled with the narrow conception of privacy. [39] In this regard, it is also normally inferred that the values that conflict with privacy (with a narrow conception) are grounded in the public interest and tend to promote important values/ basic needs like human safety, human health, and human life. [40] If so, on the basis of the narrow conception of privacy, as these values are always more important than privacy, it is assumed that preserving non-privacy values implies weakening privacy values. This might mislead us to consider that agents have a *duty* to engage in activities supporting such values to the extent that consent is not required unless an even more important value/ interest is harmed. Such a view is closer to the interest-conception than the will-conception, which I have addressed in Section 4.3.2.

[38] This can be a contingent requirement central to the alternative argument addressed in section 3.4.2.
[39] Beyleveld, 'Conceptualising Privacy in Relation to Medical Research Values' 156.
[40] Ibid 155-156.

On the other hand, on the basis of a broad conception of privacy, privacy does not merely protect one value, but several. In this regard, the broad conception of privacy implies a greater opportunity to apply the co-operative model. However, recognition of the limits of such an approach is needed.

3. Limits of the Broad Conception of Privacy

It must be noted that a broad conception of privacy is not to say that 'everything is privacy.' In other words, the conception of privacy still needs to stay within some basic characteristics of privacy. As addressed in Section 4.2.1, any discussion defending the fundamental value of privacy interests has to define the concept so as to *differentiate it from other ideas.* In this regard, logically, as there must be different ideas, the conception of privacy will never cover every value. In sum, the conception of privacy can be broad, but it still needs to be privacy rather than irrelevant conceptions e.g., the right a fair trial.

Moreover, the consequence of a broad conception of privacy is that it does not only protect one value but several. Hence, there is a second limit to the broad conception of privacy – a possibility of conflict within the co-operative model. Specifically, 'not only is privacy capable of conflicting with other non-privacy interests, but some privacy interests are capable of conflicting with each other.' [41]

There is no denying that under a broad conception of privacy, protected privacy values may still be in conflict with each other. This is similar to the idea of partnership we have already discussed: in general, partners co-operate with each other

[41] Ibid 158.

in order to *efficiently* avoid risks of violating/ take care of general interests of all the partners. However, there remains a possibility for the interests of different partners to clash. Moreover, even the interests of the same partner (agent) can come into conflict. In this regard, the criterion of degrees of needfulness for action can then be used to assess these competing values within the conception of privacy both inter-personally and intra-personally.[42]

Nevertheless, it is recalled that provided that valid consent is obtained, there is no need to deal with the subsequent substantive justification. Hence, with respect to the co-operative model, valid consent is a crucial, serving as a device to respect fundamental rights and freedoms. Specifically, if the relationship between the controller/ processor and the data subjects can be built on a basis of trust within a co-operative model, i.e., the data subjects are confident that the controller/ processor will only do *what has been agreed*, conflicts can be efficiently reduced. Methods contributing to improving the opportunity of obtaining valid consent from data subjects must therefore be evaluated and applied. This will be explored in the next subsection.

4. Consent and the Co-operative Model

On the basis of the narrow concept of privacy which is normally coupled with the conflict model, the use of personal data without consent will not necessarily involve a breach of privacy. This is because, on the basis of the conflict model, if there is any conflict between privacy and non-privacy interests, one of them must give way. If a non-privacy interest is more important than privacy (which is usually claimed by conflict model supporters), consent is not necessarily required unless the actions

[42] Ibid 158. See: Chapter 6.

protecting the non-privacy interest will result in more important generic harms. Secondly, on the basis of a narrow concept of privacy, privacy can hardly override non-privacy interests. Opposite to this, if the conflict model is coupled with the broad conception of privacy, actions protecting non-privacy values can never be undertaken without consent. However, as I have addressed above, such a relationship may generate a tension or contradiction, this circumstance can barely happen. In sum, consent plays a less crucial role in the conflict model.

On the other hand, valid consent has more opportunities to be obtained when the broad concept of privacy is adopted. Provided that consent is validly obtained, there is no conflict. Such preventive measures to improving opportunities for consent are capable of avoiding harm. This is exactly the central idea of the co-operative model. It should be noted, on the one hand, that the higher chances for consent can make the co-operative model more applicable; on the other hand, consent may work well if privacy interests cooperate with each other (coupled with the broad conception of privacy). In this respect, indeed, consent and the co-operative model cooperate. Moreover, when the procedural justification –valid consent is in play, the conflict between two interests disappears and the generic harm is avoided. It is thus no longer a ‘conflict model’ as the two interests are supporting each other. Hence, consent plays a more important role in the co-operative model rather than the conflict model.

7.2.2 Enhance the Co-operative Model

I have said in the previous subsection that, by accepting a broad conception of privacy, the co-operative model is more suitable. This subsection aims to address how to enhance the co-operative model by exemplifying two notable privacy and data

protection enhancing mechanisms which particularly engage the practicability of the co-operative model. For the purpose of this thesis, this subsection will not offer a comprehensive review of the entire framework, but will instead analyse how to couple the suggested mechanisms with the co-operative model. It is pointed out that, based on the co-operative model, the technologic-centricity and agent-centricity characteristics of such mechanisms cannot be seen as ontologically distinct matters but instead they are capable of supporting each other. In this regard, the focal point is to consolidate trust in order to improve opportunities for obtaining valid consent.

1. The Enhancement of the Co-operative Model

If there is a conflict between generic rights, harm is caused in general. The harm may be justified according to the criterion of degrees of needfulness for action. If not, then remedies may be applied. Article 23(1) of the Data Protection Directive deals with this by stating that ‘Member States shall provide that any person who has suffered damage as a result of an unlawful processing operation or of any act incompatible with the national provisions adopted pursuant to this Directive is entitled to receive compensation from the controller for the damage suffered.’

However, with the PGC in mind, it is noted that the risk of violating generic rights must be minimised in so far as it is possible to do so. In this regard, the enhancement of the co-operative model can be used to effectively minimise the risk of violating the right to privacy.

In terms of ethical or privacy issues with respect to the development of new technologies, risks could be more easily assessed in the initial stages such as the

designing period since any control or change is more difficult when a technology has become more deeply entrenched.[43] However, with reference to the Collingridge dilemma,[44] impact is difficult to predict at the early stage.[45] To deal with this, privacy and data protection issues need to be assessed early on with not only the expert assessment of data controllers, e.g., policy makers/ inventors in the public domain as well as private enterprises, but also with the involvement of the data subjects and supervisors. This dilemma calls for an early engagement, e.g., mutual communication and dialogue in a 'codes of conduct' form,[46] involving every participant of the data processing, which mirrors the spirit of the co-operative model. With this in mind, early privacy and data protection intervention in the research and innovation of science and technology process can 'help to avoid that technologies fail to embed in society and or help that their positive and negative impacts are better governed and exploited at a much earlier stage.'[47] In this respect, appropriate risk assessment is definitely part of the procedure towards 'healthy' types of scientific and technological developments, which can avoid (at least to some extent) subsequent conflicts between the interest of the progress of research and the values of privacy and data protection. This is in line with the idea that the risk of violating the PGC must be minimised in so far as it is possible to do so. Accordingly, it is plausible to argue that a legal standard 'applicable to European privacy and data protection legislation' should be established

[43] René von Schomberg, 'Introduction: Towards Responsible Research and Innovation in the Information and Communication Technologies and Security Technologies Fields' in René von Schomberg (ed), *Towards Responsible Research and Innovation in the Information and Communication Technologies and Security Technologies Fields* (Publications Office of the European Union 2011) 8.
[44] David Collingridge, *The Social Control of Technology* (Palgrave Macmillan 1981).
[45] Schomberg (n 44) 8.
[46] Codes of conduct, as Menevidis and others argue, are particular rules/ guidelines to individuals when dealing with themes concerning ethical values in relation to researches and innovations of science and technology, e.g., biometric data processing. For details, see: Zaharya Menevidis, Samantha Swartzman and Efstratios Stylianidis, 'Code of Conduct for FP7 Researchers on Medical and Biometric Data Privacy' in René von Schomberg (ed), *Towards Responsible Research and Innovation in the Information and Communication Technologies and Security Technologies Fields* (Publications Office of the European Union 2011) 116-132.
[47] Schomberg (n 44) 9.

and followed on the basis of such reasoning.[48]

With a view to avoiding harm, both prevention and precaution relate to risk assessment and anticipation of harm at an early stage. However, there is a need to distinguish prevention and precaution.[49] It is noted that risk assessment includes two types of risks, namely the identified and uncertain ones. It has been argued that preventive measures 'take place when there are identifiable risks,' while precaution is supposed to deal with uncertain risks.[50] For example, in terms of the precautionary principle, it is mentioned in Article 174 of the Treaty of Amsterdam (now Article 191 TEFU), which was the first provision to incorporate the precautionary principle into the environment policy of the EU, that '[t]he Contracting Parties shall apply the precautionary principle, where to take preventive measures when there is reason to assume that substances or energy introduced... *when there is no conclusive evidence* of a causal relationship between inputs and their alleged effects.' (emphasis added)

Moreover, to assess risks in both preventive actions and precautionary assessments, the possibility of risk should be understood in a broad sense in order to ensure a higher level of protection of generic rights. To accept a broader conception of privacy enables us to achieve the purpose of evaluating risks in this context. As Warren et al. address, 'PIAs have to consider privacy risks in a wider framework that takes into account the broader set of community values and expectations about privacy.'[51] Again, this is in line with the justification of the co-operative model.

[48] Luiz Costa, 'Privacy and the Precautionary Principle' (2012) 28 Computer Law & Security Review14.
[49] Ibid 16.
[50] Ibid 16.
[51] Adam Warren and others, 'Privacy Impact Assessments: International Experience as a Basis for UK Guidance' (2008) 24 Computer Law & Security Review 235.

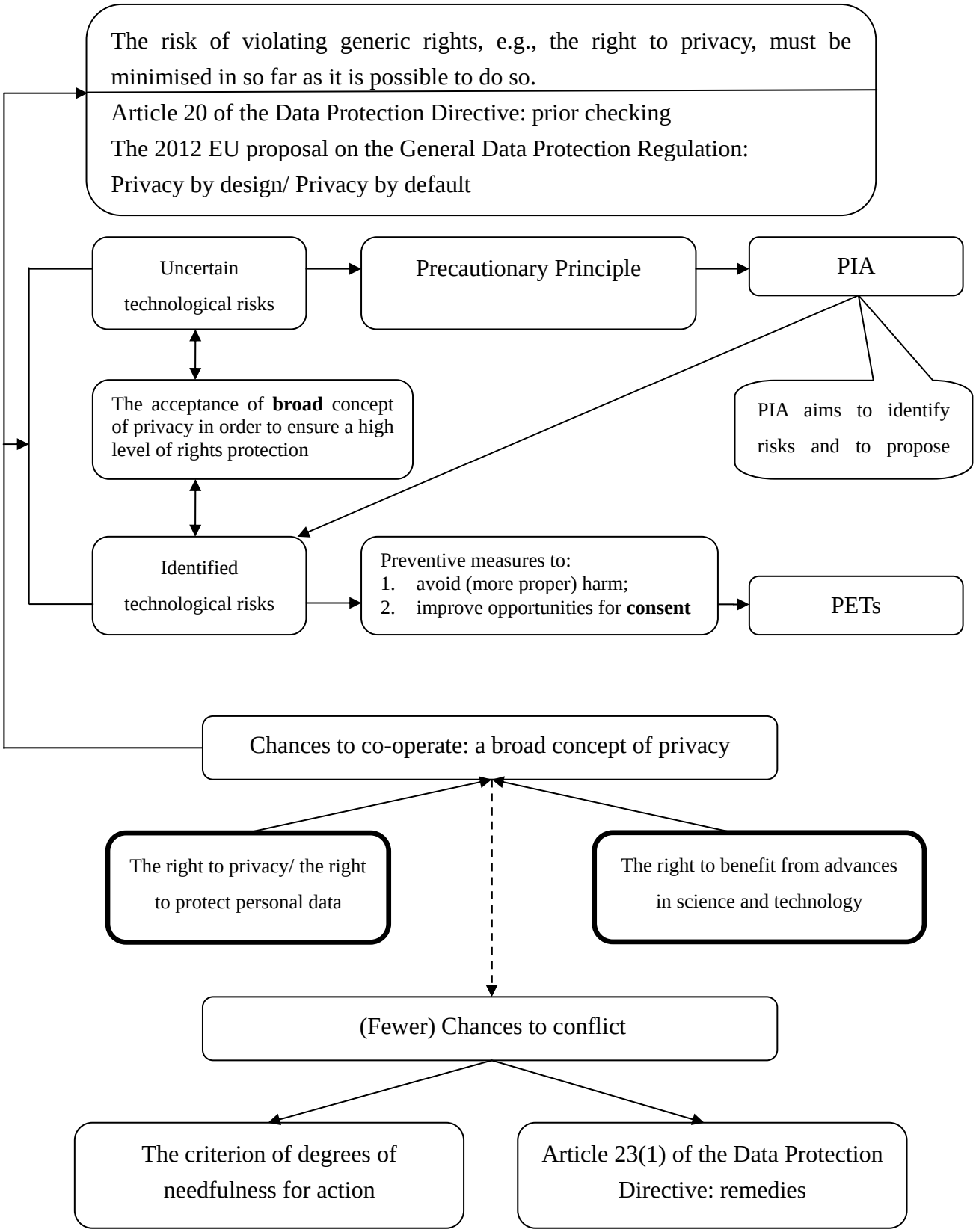
Although Article 20(1) of the Directive provides a prior checking approach,[52] as Costa observes, unlike Article 2 of Directive 85/337/EEC,[53] there is no specific provision offered. I argue that, in light of uncertain risks, in order to adopt the precautionary principle to deal with harms to the right to privacy and the right to protect personal data, it is better to enhance the co-operative model by applying the Privacy and Data Protection Impact Assessment (PIA).[54] On the other hand, when dealing with specific and identified risks, Privacy Enhancing Technologies (PETs) which adopt a 'privacy by design' idea are more appropriate.

[52] It states: 'Member States shall determine the processing operations likely to present specific risks to the rights and freedoms of data subjects and shall check that these processing operations are examined prior to the start thereof.'

[53] Suggesting the environmental impact assessment, Articles 2(1) and 2(2) of the Directive state that 'Member States shall adopt all measures necessary to ensure that, before consent is given, projects likely to have significant effects on the environment by virtue inter alia, of their nature, size or location are made subject to an assessment with regard to their effects,…' and 'The environmental impact assessment may be integrated into the existing procedures for consent to projects in the Member States, or, failing this, into other procedures or into procedures to be established to comply with the aims of this Directive.'

[54] Cf. Recital 70 of the proposed EU General Data Protection Regulation: '…such indiscriminate general notification obligation should be abolished, and replaced by effective procedures and mechanism which focus instead on those processing operations which are likely to present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes. In such cases, a data protection impact assessment should be carried out by the controller or processor prior to the processing, which should include in particular the envisaged measures, safeguards and mechanisms for ensuring the protection of personal data and for demonstrating the compliance with this Regulation.'

Figure 7.1: A Brief Structure of the Co-operative Model



2. Privacy Impact Assessment

To understand PIA, it is better to begin by looking at the social and ethical intervention in compliance with fundamental rights and freedoms in research and innovation of science and technology. The term 'responsible research and innovation' refers to[55]

> transparent, interactive process by which societal actors and innovators become mutually responsive to each other with a view on the (ethical) acceptability, sustainability and societal desirability of the innovation process and its marketable products (in order to allow a proper embedding of scientific and technological advances in our society).

This definition suggests proposals beyond scientific and technological excellence which should include a social and ethical review.[56] In this regard, the conduct of collective collaboration between researchers/ inventors and social scientists is desirable. This is close to the definition of an instrument of risk governance, i.e., PIA:[57]

> a process of engaging stakeholders in order to consider how privacy might be impacted by the development of a new technology, product, service, project or policy and what measures could be taken to avoid or mitigate unwanted effects.

The advantage of the use of PIA is to 'reduce the human cost of trial and error and

[55] Schomberg (n 44) 9. The justification of responsible research and innovation can be found at: ibid 8-9.
[56] Ibid 10. For detailed discussions on responsible research and innovation including its concept, limits and applications, see: Bernd Carsten Stahl, 'IT for a Better Future. How to Integrate Ethics, Politics and Innovation' in René von Schomberg (ed), *Towards Responsible Research and Innovation in the Information and Communication Technologies and Security Technologies Fields* (Publications Office of the European Union 2011) 28-31.
[57] Wright and others (n 12) 84.

make advantage of a societal learning process of stakeholders and technical innovators.'[58] Indeed, this methodology of risk management is by no means a new idea. For example, it was reviewed by the WP29.[59] The proposed framework aims to assist the Member States as well as their citizens and third parties in addressing privacy and data protection risks as required by EU Directives, in particular the Data Protection Directive. It is expected to achieve its purpose by taking appropriate actions, i.e., 'a close examination of the cost and benefits of specific security and privacy-related risks'[60] in order to prevent, or at least minimise, the negative impact of the biometric and RFID systems as well as the deployment of their applications. In this regard, the suggested PIA has to be consistent with the data protection requirements set out by the EU and the ECHR standard given/ interpreted by the ECtHR.

The WP29 is not the only EU authority or consolation party who noticed the necessity of PIA. The European Parliament, in its resolution on Passenger Name Records (PNR), also noticed that 'any new legislative instrument must be preceded by a Privacy Impact Assessment and a proportionality test,…' [61] There are other indications of a growing interest in PIA. Viviane Reding, Vice-President of the

[58] Schomberg (n 44) 10.
[59] It should be noted that PIA reviewed by the WP29 is specifically for the RFID applications. See: Article 29 Data Protection Working Party, *Opinion 5/2010 on the Industry Proposal for a Privacy and Data Protection Impact Assessment Framework for RFID Applications* (No 00066/10/EN, WP175, 2010) and Article 29 Data Protection Working Party, *Opinion 9/2011 on the Revised Industry Proposal for a Privacy and Data Protection Impact Assessment Framework for RFID Applications* (No 00327/11/EN, WP180, 2011). It should be noted here that the main critique on the first version of the proposed framework addressed by the first opinion is the concern over the fails to 'invite the RFID operator to assess privacy and data protection issues that could arise when tags are carried by individuals in everyday life.' This leads to the revised version of the framework. See: Article 29 Data Protection Working Party, *Opinion 5/2010 on the Industry Proposal for a Privacy and Data Protection Impact Assessment Framework for RFID Applications* 9. For a general overview, see: Laurie and Sethi (n 15) 48, 59.
[60] Communication form the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, *Radio Frequency Identification (RFID) in Europe: steps towards a policy framework*, COM (2007) 96 final 6.
[61] European Parliament, Resolution of 5 May 2010 on the launch of negotiations for Passenger Name Record (PNR) agreements with the United States, Australia and Canada. OJ 2011/C 81 E/12.

European Commission responsible for Justice, Fundamental Rights and Citizenship, for example, remarked in July 2010 that 'businesses and public authorities… will need to better assume their responsibilities by putting in place certain mechanisms such as the appointment of Data Protection Officers, the carrying out of Privacy Impact Assessments and applying a 'Privacy by Design' approach.'[62] Moreover, the International Organization for Standardization (ISO) has also offered a standard for PIA in the field of financial services.[63]

PIA defined in the framework assessing RFID applications is organised as follows.[64] First, there is a 'pre-assessment (initial analysis) phase', which classifies the application basis on a 4-level scale.[65] This allows to determine whether later stages of PIA are needed or not. Secondly, a four-step risk assessment phase is suggested: (1) to characterise the application; (2) to identify the risks of personal data in terms of privacy and compliance with European data protection law regime; (3) to identify and recommend controls; and (4) to document the detailed results of PIA in reports.

This concerted co-operation is crucial in the design of technology early on. Indeed, the idea of '**privacy by design**', which indicates the concept of 'embedding privacy proactively into technology itself,'[66] has been noticed in a European

[62] Viviane Reding, 'Towards A True Single Market of Data Protection (SPEECH/10/386, Meeting of the Article 29 Working Party, Review of the Data protection Legal Framework)' (*The EU*, 2010) <http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/10/386> accessed 24 April 2012.
[63] International Organization for Standardization, 'ISO 22307:2008: Financial services -- Privacy impact assessment, 16 Apr 2008.' (2008) <http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=40897> accessed 20 Februrary 2012.
[64] Article 29 Data Protection Working Party, *Opinion 9/2011 on the Revised Industry Proposal for a Privacy and Data Protection Impact Assessment Framework for RFID Applications* 4-5.
[65] Ibid 4. Also, the appendix of the opinion, 6-7.
[66] Article 29 Data Protection Working Party, *Opinion 3/2012 on Developments in Biometric Technologies* (No 00720/12/EN, WP193, 2012) 28.

Commission proposal on a major legal reform of data protection rules in early 2012.[67] In the proposed Article 19(2) of the new Directive, it is set out that the Member States must ensure the compliance of the controller with the obligations to 'adopt policies and implement appropriate measures, which meet in particular the principles of data protection by design and data protection by default.'[68]

In this regard, the 'privacy by design' concept of PIA can be understood as follows:

(1) Help data controllers:

a. To address privacy and data protection issues *before* the technological applications have been deployed. This is able to save a considerable amount of cost on amending the services and products affecting privacy concerns.[69]
b. To assess privacy risks, find out 'technical and organisational measures' against harms and protect rights set forth by the data protection principles. By doing so, this can also assist data controllers to 'gain more insight' into the privacy and data protection issues regarding the applications.[70]
c. To build/ improve the trust afforded by data subjects. This enables data controllers to collect and process personal data more easily and accurately.

[67] European Commission, 'Commission Proposes A Comprehensive Reform of the Data Protection Rules' (2012) <http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm> accessed 30 Janurary 2012.
[68] Recital 38 of the proposed Directive. European Commission, 'Proposal for A Directive of the European Parliament and of the Council on the Protection of Individuals with regard to the Processing of Personal Data by Competent Authorities for the Purposes of Prevention, Investigation, Detection or Prosecution of Criminal Offences or the Execution of Criminal Penalties, and the Free Movement of Such Data, (COM(2012) 10 final)' (2012) <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0010:FIN:EN:PDF> accessed 30 Janurary 2012.
[69] Article 29 Data Protection Working Party, *Opinion 5/2010 on the Industry Proposal for a Privacy and Data Protection Impact Assessment Framework for RFID Applications* 5.
[70] Ibid 5.

This leads to a higher chance for data subjects to consent. In this regard, there will not be a violation of the rights considered. The relationship between data subjects and controllers in this aspect will be further discussed together with the next measure enhancing the co-operative model.

(2) Help data subjects:

a. To secure and strengthen their ability to exercise their privacy and data protection rights.
b. To enjoy the benefits of scientific and technological applications at a lower cost. This is because the manufacturing costs/ risks of the industries have been reduced to some extent for the reasons set out above, and the consumers thus *may have the chance* to share the gained profits.

Additionally, the data protection authorities (DPAs) can identify best practices regarding the way data protection is implemented by private industries and public authorities. Hence, the privacy by design characteristic implies technology is left in the hands of main parties of data processing. In this regard, PIA can be a useful means to simplify the process for data subjects, data controllers and DPAs 'in monitoring potential privacy risks prior to the implementation of *any* particular model.' [71] (emphasis added) More importantly, such approach is decisive for establishing an environment based on trust. [72] Indeed, PIA not only increases the possibility of

[71] Laurie and Sethi (n 15) 59. It is noted that the prior risk assessment measures are not applied by every legal regimes. However, risk analysis measures are needed to obtain an effective set of security instrument. See: G.W. van Blarkom, J.J. Borking and P. Verhaar, 'PET' in G.W. van Blarkom, J.J. Borking and J.G.E. Olk (eds), *Handbook of Privacy and Privacy-Enhancing Technologies - The case of Intelligent Software Agents* (College bescherming persoonsgegevens 2003) 45.
[72] 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

avoiding conflicts of interest, by building public trust, it also '[a]chieving a better balance among conflict interests.'[73] Overall, a *well-designed* PIA can pragmatically reflect the promises of the co-operative model.

3. Privacy Enhancing Technologies

PETs have been defined as a system of the Information and Communication Technology (ICT)[74] that protects privacy, in particular informational privacy and personal identity. They aim to minimise the unnecessary collection and processing of personal data altogether, or gives direct control over revelation of personal data to the agent concerned, without the unbearable loss of the functionality of the ICT.[75] The application, according to Burkert, must be distinguished from those data security technologies seeking to 'render data processing safe regardless of the legitimacy of processing.'[76] This is because PETs emphasise that personal data can only be collected if necessary in the very first place.[77] This reflects the fact that the security of personal data is not the only data protection principle. PETs should, therefore, take the overall data principles into account.

'Privacy by design' is a crucial basis for the successful application of PETs.[78]

---

policy framework' COM(2007) 96, paragraph 52, OJ 2008/C 101/01.
[73] Wright and others (n 17) 90.
[74] See: Chapter 2.
[75] Herbert Burkert, 'Privacy-Enhancing Technologies: Typology, Critique, Vision' in Philip E. Agre and Marc Rotenberg (eds), *Technology and Privacy: The New Landscape* (MIT Press 1998) 125; Dag Wiese Schartum, 'Designing and Formulating Data Protection Laws' (2010) 1 International Journal of Law and Information Technology20; Colin Bennett and Charles Raab, *The Governance of Privacy: Policy Instruments in Global Perspective* (MIT Press 2006) 141; John J. Borking, 'Why Adopting Privacy Enhancing Technologies (PETs) Takes so Much Time' in Serge Gutwirth and others (eds), *Computers, Privacy and Data Protection: an Element of Choice* (Springer 2011) 309-310; and Blarkom, Borking and Verhaar (n 72) 33.
[76] Burkert (n 76) 125.
[77] Bennett and Raab (n 76) 141.
[78] Ronald Koorn and others, *Privacy Enhancing Technologies –White Paper for Decision-Makers*

This characteristic, as we have seen, fits in with the co-operation model. Additional attention is directed to the requirement of the design of PETs to provide user protection against discovery and misuse of individual identity, namely: (1) pseudonymity; (2) anonymity; (3) unlinkability; and (4) unobservability.[79] The implementation of PETs should firstly identify what kind of risk in relation to privacy they are designed to protect.[80] Once this is identified, a number of creative further processes can be developed. For example, biometrics is one of the possibilities of using PETs.[81] Moreover, there are options, composed of technologies divided in four categories presenting different characters of design, positioned with respect to different levels of effectiveness of the protection of privacy.[82]

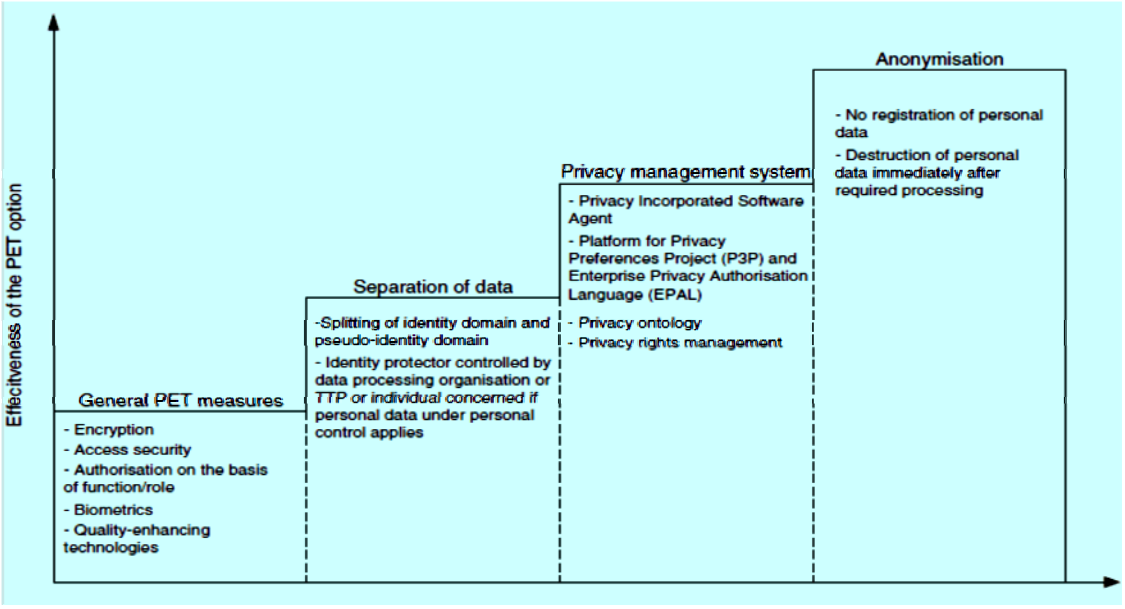


Figure 1: Effectiveness of different options of PETs[83]

(2004) 3.

[79] Blarkom, Borking and Verhaar (n 72) 47-49.

[80] Ibid 37-38.

[81] Seven principles/ types of the PET developments have been listed by Blarkom, Borking and Verhaar, namely: (1) limitation in the collection of personal data; (2) identification/ authentication/ authorisation; (3) standard techniques used for privacy protection; (4) pseudo-identity; (5) encryption; (6) biometrics; and (7) audit ability. Ibid 37-42.

[82] Borking (n 76) 310-311.

[83] Koorn and others (n 79) 33 < http://www.dutchdpa.nl/downloads_overig/PET_whitebook.pdf >,

To reflect the privacy by design line of reasoning, two approaches have been presented.[84] First, the 'engineer-oriented' approach takes the enhancement of catering for the privacy dimension into account to offer standards and guidelines for IT security.[85] Secondly, the "market-oriented" approach stresses elements including 'self-regulation, audit schemes and quality seals.'[86] Examples of live applications of PETs can be found in a variety of sectors, e.g., higher education,[87] health sector,[88] social security network,[89] transportation,[90] and anonymous service.[91]

These four concepts which enable securing identity protection of personal data (but should not be viewed as confined to personal identity protection), however, do not necessarily protect privacy. The reasoning behind this argument goes as follows.

1. Under *the broad conception of privacy* adopted in the co-operation model, a right to know the personal implications for oneself of the advance of science and technology arguably exists under the right to privacy, but is rendered impossible by the design of PETs.

   Individuals, arguably, have a privacy right for the developments of science and technology to be conducted. This is because the enjoyment of such

---

accessed 8th February 2012. Also cited by Borking (n 76) 311. TTP in the figure means Trusted Third Party, which is a separated database. It should be noted that the staircase here does not represent a growth model but options depending on the 'individual situation.' Ibid 310.

[84] Walter Peissl, 'Responsible Research and Innovation in ICT: The Case of Privacy' in René von Schomberg (ed), *Towards Responsible Research and Innovation in the Information and Communication Technologies and Security Technologies Fields* (Publications Office of the European Union 2011) 39-42.

[85] Ibid 39.

[86] Ibid 39.

[87] E.g. the Higher Education Clearinghouse (StudieLink). Koorn and others (n 79) 8.

[88] E.g. the National Central Medication Registration (LCMR system), National Trauma Information System (NTIS) in the Netherlands, hospital information system, and online medical history file. Ibid 10, 22, 26, 61.

[89] E.g. RINIS Clearinghouse and Suwinet systems in the Netherlands. Ibid 13, 24.

[90] E.g. road pricing system and transport smart card. Ibid 27, 56.

[91] E.g. the AgeKey system to prove the age to purchase tobaccos in the Netherlands and electronic voting. Ibid 31, 36.

developments can also improve private life. However, it is noted that the less useful the results, the weaker the justification for such developments in science and technology. Anonymised data, for example, is less valuable for such science and technology than the non-anonymised data. Therefore, the concept of privacy in relation to the enjoyment of science and technology might not be protected.[92]

2. It is common to assume that technology remains stable and performs as intended across time and space. This perspective which puts technology in the centre is termed the 'techno-centric' view by Gürses and Berendt.[93] However, two technical facts must be pointed out. First, there is no trust with regards to the internet.[94] Accordingly, the effectiveness of biometric applications may be overestimated if without proper consultation with technical experts. For example, with reference to the introduction of biometric passport in the Netherlands, engineers – and not politicians - warned that:[95]

> The effectiveness of biometry is highly overrated, especially by politicians and policy makers. Despite rapid growth in applications, the large-scale use of biometry is untested. The difficulty is that it is not only unproven in a huge single application (such as e-passports), but also not with many different applications in parallel... The interference caused by the diversity of applications—each with its own security policy, if any—may lead to

[92] Cf. Deryck Beyleveld, 'Is consent necessary and/ or sufficient to authorise medical database research?' (Regulation and Governance of Medical Database Research in the United Kingdom, Sheffield, 17th June 2011).
[93] Seda Gürses and Bettina Berendt, 'PETs in the Surveillance Society: A Critical Review of the Potentials and Limitations of the Privacy as Confidentiality Paradigm' in Serge Gutwirth, Yves Poullet and Paul De Hert (eds), *Data Protection in a Profiled World* (Springer 2010) 302.
[94] Ibid 307.
[95] Jaap-Henk Hoepman and others, 'Crossing Borders: Security and Privacy Issues of the European e-Passport' (2006) 4266 Lecture Notes in Computer Science 152-167.

unforeseen forms of fraud.

Secondly, the protection through the confidentiality of personal data emanating from individuals is limited in scope.[96] Hence, arguably, it is unrealistic to expect that technical methods can actually keep personal data confidential and in line with *all* data protection principles.

Both of the problems can be addressed by improving opportunities for consent and enhancing its substance. In the first case, by obtaining consent (with respect to waive the right to know the personal implications for oneself of the advance of science and technology), there is no need for substantive justification. It is thus noted that *technologies which can achieve this purpose are also PETs*.[97]

In the second situation, it is suggested that a human-centric model which concentrates on 'how humans make sense of and interact with technology in various circumstances'[98] should also be taken into account. This is not forbidden by the PGC since this approach considers human beings/ agents as an end rather than the method through which to develop technology. The approach indicates that PETs and social practices (in a human-centric sense) can be seen as supporting each other. In this light, it is suggested that PETs alone cannot be enough to satisfy the need of the accountability of the data subjects. For example, accountability in relation to the use of anonymous data for transparency instruments and the avoidance of data abuses should be considered.[99] Moreover, a study on the basis of empirical evidence has shown that anonymising data may still result in specific concerns over the mistrust of

[96] Gürses and Berendt (n 94) 307.
[97] Beyleveld, 'Is consent necessary and/ or sufficient to authorise medical database research?'.
[98] Gürses and Berendt (n 94) 302-303 cited from Wanda J. Orlikowski, 'Sociomaterial Practices: Exploring Technology at Work' (2008) 28 Organization Studies 1435-1448.
[99] Gürses and Berendt (n 94) 315.

data controllers of the public and private sectors.[100] Accordingly, as Koorn et al. suggest, proper applications of PETs require an effective foundation of organisational management,[101] e.g., Identity and Access Management (IAM), which minimise the process, use and access to sensitive personal data[102] such as biometric data.

Overall, the focal point of the practicability of enhancing the co-operative model falls on the improvement of opportunities for valid consent regarding all participants of personal data collection, processing and use. To achieve this purpose, the suggested instruments include enhancing the ability to trust, positive experiences, predictable performances, comprehensive transparent information, shared values, better communications and interface designs.[103] In this light, technologies improving opportunities for consent and enhancing its meaningfulness are also PETs.[104] We must, in addition, take into account the best social practices that we can gather, avoiding the risk of applying the techno-centric model alone. This includes a series of pragmatic guidelines and practices. Once such mechanisms are defined, for example, States should ensure that the biometric data controllers and the RFID operators will ensure the mechanisms are contextualised in the competent institutional frameworks such as the DPAs. This shall be discussed in the following section.

---

[100] Gill Haddow and others, ''Nothing Is Really Safe': A Focus Group Study on the Processes of Anonymizing and Sharing of Health Data for Research Purposes' (2011) 17 Journal of Evaluation in Clinical Practice 1140-1146.

[101] Koorn and others (n 79) 46-51. In this respect, a 'sandwich of technologies' model in combination of strategies including the prevention of identification, the guarantee against unlawful processing of personal data and the application of specific technologies to enhance privacy. Ibid 48-49. Also, Directorate-General Justice European Commission, Freedom and Security,, 'Comparative Study on Different Approaches to New Privacy Challenges, in Particular in the Light of Technological Developments' (2010) <http://ec.europa.eu/justice/policies/privacy/docs/studies/new_privacy_challenges/final_report_en.pdf> accessed 30 Janurary 2012, 49-50.

[102] Borking (n 76) 322-327.

[103] L. Korba, A. Patrick and R. Song, 'Trust model and network aspects' in G.W. van Blarkom, J.J. Borking and J.G.E. Olk (eds), *Handbook of Privacy and Privacy-Enhancing Technologies - The case of Intelligent Software Agents* (College bescherming persoonsgegevens 2003) 157-161.

[104] Beyleveld, 'Is consent necessary and/ or sufficient to authorise medical database research?'.

7.3 Operationalising the PGC and the Co-operative Model

7.3.1 Regulating Technology?

To address the regulatory guidelines of sophisticated technologies at stake, two questions must be posed: first, whether and why should such technologies be regulated; secondly, if they should be regulated, how to provide guidelines to determine an adequate regulation of the technology at hand.

In light of biometric technologies, a number of points previously raised in this thesis should be recalled when looking at the first question. It was pointed out that, on the basis of the rule-preclusionary conception of property, an agent has a *prima facie* right to her biometric samples. In addition, the agent also has a *prima facie* right to subsequent applications of her samples, subject to her consent to waive the benefit of the right or the overriding of competing rights.[105] To begin, I will discuss the regulatory tendency in relation to biometric samples and their subsequent applications. Following the discussion, attention will be then directed to the importance and proposed guidelines of principled and proportionate governance.

By accepting the rule-preclusionary conception of property, the removal of biometric samples without any attempt to abandon it implies an agent's retaining of rule-preclusionary control over the material.[106] This includes positive and negative rights. To protect such a generic right as well as other overlapping generic rights e.g., the right to privacy from the insidious threat to the way an agent acts (as we have

[105] Section 6.3.1.
[106] Shaun D. Pattinson, 'Directed Donation and Ownership of Human Organs' (2011) 31 Legal Studies 407.

addressed in Chapter 2),[107] it is at least arguable that there is a demand to determine adequate regulations. However, there might be different responses to this argument. For example, whenever new and powerful technologies have been developed to the point of being able to be widely applied and implemented, there will be opponents holding differing opinions. This is termed the 'Luddite argument' by Solove.[108] Privacy and data protection advocates, for example, may be labelled as the Luddites. However, this can be rebutted by the 'Titanic Phenomenon', which holds that while many new technological proposals have great advantages, 'proponents are not giving adequate thought to the consequences if they fail.'[109]This phenomenon, pointed out by Solove, refers to the tendency of those 'quick' users of the changing technologies: they tend to be overconfident or optimistic to apply the technology without 'appropriate legal architecture in place to use it responsibly.'[110]

Another response is to abandon regulation and assume that technological prospects might/ be able to dictate the 'right direction' or to try at least to 'hold the regulatory line, concentrating resources on the most serious violations.'[111] These responses seem to be quite plausible within the free-market model as discussed in Chapter 6.

Nevertheless, as we have also seen, the minimal-regulation model may not be adequate. For example, in terms of serious threats, Fukuyama considers that such

[107] Under a broad concept of privacy, the rule-preclusionary control over the material and data is arguably included by privacy.
[108] Solove (n 16) 201. Luddites is a term originally means those who protested against the mechanisation of the Industrial Revolution in 19th century. Similarly, Beyleveld and Pattinson term this 'science hatred,' meaning the belief that science is inherently evil. Deryck Beyleveld and Shaun D. Pattinson, 'Individual Rights, Social Justice, and the Allocation Of Advances in Biotechnology' in Michael Boylan (ed), *Public Health Policy and Ethics* (Kluwer 2004) 70.
[109] Solove (n 16) 199. The 'Titanic Phenomenon' indicates that the designers and builders of the Titanic did not provide enough lifeboats since they thought the ship is unsinkable.
[110] Ibid 203.
[111] Roger Brownsword, *Rights, Regulation, and the Technological Revolution* (OUP 2008) 315.

technologies cannot be captured by the Utilitarian calculus.[112] Indeed, the principle of priority of consent and data protection practice are appreciated and encouraged in the Gewirthian approach. The theoretical framework granting generic conditions of agency does not, however, by itself, articulate much about the morality of the techniques of regulating subsequent applications of biometric samples.

Regulating technology with respect to privacy and data protection issues encounters a more specific problem: the scope and the conception of personal data are influenced by rapidly changing technology and data-sharing practices. This is because the line between personal data and non-personal data – whether the data can be identified/ identifiable – profoundly depends on technology. The scope of personal data may expand since changing technologies provide stronger and more efficient abilities to identify and re-identify data. In this regard, Paul Ohm argues that the scope of personal data[113] 'will never stop growing until it includes everything.'[114] For example, it is pointed out in the press release on the 2012 reform of the EU data protection system that '[t]echnological progress and globalisation have profoundly changed the way our data is collected, accessed and used'[115] and the cloud computing has been noted in particular as a specific type of new challenge.[116] Ohm thus proposes an alternative approach to focus the privacy law on a different conception of personal data; the regulators should

[112] Francis Fukuyama, *Our Posthuman Future* (Profile Books 2002) 101, citing from Brownsword (n 112) 314.
[113] It seems that Ohm does not distinguish ideas between personal data and personally identifiable information (PII). Paul Ohm, 'Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization' (2010) 57 UCLA Law Review 1704.
[114] Ibid 1742.
[115] European Commission, 'Commission Proposes A Comprehensive Reform of the Data Protection Rules' 1.
[116] European Commission, 'How Will the EU's Reform Adapt Data Protection Rules to New Technological Developments?' (2012) <http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/8_en.pdf> accessed 30 Janurary 2012.

> …consider a series of factors to identify situations in which harm is likely and whether it outweighs the benefits of unfettered information flow. When they identify harm that outweighs these benefits, they should regulate, focusing on narrow contexts and specific sectors rather than trying to regulate broadly across industries.[117]

Again, this resonates with the Utilitarian argument and therefore can be rebutted through the objections presented above. Moreover, the approach suggested by Ohm is to

> …resign themselves to a world with less privacy than they would like. But more often, regulators should prevent privacy harm by squeezing and reducing the flow of information in society, even though in doing so they may need to sacrifice, at least a little, important counter values like innovation, free speech, and security.[118]

However, this approach faces the objections stemming from the European data protection model, which consider the protection of the flow of information as the primary purpose of the Data Protection Directive. As we have seen, this purpose may not come into conflict with privacy values. Indeed, Solove comments that 'where the first step is to restrict the flow of information is a move in the wrong direction.'[119]

Nevertheless, it should be noted that in practice some measures suggested by Ohm, may still have their merits. For example, he suggests the regulators should 'incorporate risk assessment strategies that deal with the reality of easy

[117] Ohm (n 114) 1759.
[118] Ibid 1706.
[119] Paul M. Schwartz and Daniel J. Solove, 'The PII Problem: Privacy and A New Concept of Personally Identifiable Information' (2011) 86 NYU Law Review 1868.

reidentification as the old PII model never could.'[120]

As regards the choice between the European model (which regulates all forms of data collection, processing, and using in the absence of specific exemptions) and the American model (which is based on the primacy of freedom of information, whereby unless something fits the scope of specific regulations, it is not protected),[121] having taken into account the problems of the minimal-regulation model, I contend that the European model should be favoured. Indeed, it has been suggested in a comparative study submitted to the European Commission:[122]

> Data protection law in the EU (in all areas covered by the previous three pillars) can and should continue to rest on the basic data protection principles and –criteria set out in Directive 95/46/EC. The application of these broad standards needs to be clarified (as further discussed below, in particular in sub-section V.4), but they themselves do not require major revision in order to meet the new challenges. On the contrary, they reflect European and national constitutional/human rights standards of the kind just mentioned, that need to be strongly re-affirmed.

It is noted that in the 2012 EU data protection reform proposal, a single set of rules has been suggested.[123] This is, accordingly, consistent with the European data protection model.

Moreover, Solove also suggests that, considering the problem in relation to the

[120] Ohm (n 114) 1759.
[121] Section 5.1.
[122] European Commission, 'Comparative Study on Different Approaches to New Privacy Challenges, in Particular in the Light of Technological Developments' 21.
[123] European Commission, 'Commission Proposes A Comprehensive Reform of the Data Protection Rules' 2. European Commission, '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)' (2012) <http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf> accessed 30 Janurary 2012.

gap between the law and changing technologies,[124] the '[l]aws must have sufficient breadth and flexibility to deal with rapidly evolving technology.'[125] In this regard, his 'broad principle approach' is in line with the European model.[126]

7.3.2 Regulatory Design: A General Regulatory Position

Different legal regimes may provide a variety of levels of protection against parts of the human body according to their relationship to an agent.[127] What kind of regulatory design should we consider then?

A number of complex desiderata have to be taken into account.[128] For a start, let us consider the flexibility of this regulatory instrument. It has been argued that for those rights and interests to be given equally through universal access, universal denial, or completely random allocation.[129] For those will not qualify as earth-shaking matters of justice or morality on the Gewirthian ground (at least for those does not prohibited by the PGC), a lighter form of regulation may be adequate. As regards the rights and interests that cannot be granted equally and those that present a clear violation of the generic conditions of agency, on the other hand, a more stringent regulation would be *proportionally* more suitable.

It is noted that scientifically sound and ethically robust techniques are in the

[124] Indeed, there is also a gap between legal privacy regulations and privacy practices since 'practices often do not follow the written rules.' Guagnin, Hempl and Ilten (n 12) 100.
[125] Solove (n 16) 170.
[126] Ibid 170-173.
[127] Pattinson, 'Directed Donation and Ownership of Human Organs' 406. Also, Article 29 Data Protection Working Party, *Opinion 3/2012 on Developments in Biometric Technologies* 28.
[128] In Brownswords' *Rights, Regulation, and the Technological Revolution*, he adopts Trebilcock and Iacobucci's opinion that a number of values may be in a tension. These values include: independence, accountability, expertise, detachment, transparency, confidentiality, efficiency, due process, predictability, and flexibility. See: Brownsword (n 112) 299.
[129] See section 6.2.

interest of all agents. Indeed, under a broad conception of privacy, both values can be encompassed by privacy. The rights of agents should be respected with adequate privacy and data protection practices. In the light of the technologies at hand, due to the sensitive nature and higher potential risks towards the right to privacy and data protection, a 'burdensome' regulatory position (as Utilitarian or supporters of the free-market model see it)[130] is considered by the thesis.

Based on the PGC, considerations with respect to consent are prioritised. This is particularly important when considering the conflicts between crucial rights according to the hierarchy of generic conditions of agency. This is because although conflicts can be reconciled according to the criterion of degrees of needfulness for action, a generic harm has been done (although it can be justified). By possessing valid consent, on the other hand, no violation is caused. Hence, for a rigid regulatory design, attention should be firstly paid to consent without falling into the error of the Fallacy of Necessity and Fallacy of Sufficiency.

However, in modern pluralistic communities, the idea of governance by consent may not be practical since such a consent-utopia is more likely to appear in a city-state with direct democracy.[131] The efficiency and validity of consent is, therefore, crucial for the regulatory design: by obtaining valid consent in a relatively efficient way, the tendency and possibility for a community to insist on emphasising consent can be expected and achieved. Indeed, in the proposed EU 2012 General Data Protection Regulation, in terms of consent, there is a requirement of 'explicit', which aims to 'avoid confusing parallelism with 'unambiguous' consent and in order to have one single and consistent definition of consent…'[132] Beyleveld and Brownsword have,

[130] Brownsword (n 112) 300.
[131] Deryck Beyleveld and Roger Brownsword, *Consent in the Law* (Hart Publishing 2007) 359.
[132] European Commission, 'Proposal for a Regulation of the European Parliament and of the Council

in this regard, offered a number of rather clear considerations and comments including: subjects of consent, the signalling of consent, unforced will to choose, the information for consent, reasonable interpretation, and the negation of consent.[133]

I argue that the trust between the giver and the receiver of consent penetrates through the texture of all themes presented above. The following points thus should be taken into consideration in developing a framework for the proposed regulatory design.

1. Respect for User and Controller

It has been observed that one of the new trends of biometric use is the potential to collect and analyse personal data remotely 'without the need of cooperation or action required from the individual.' RFID (including NFC) is definitely a mature selection among such covert techniques. This kind of secret but potentially non-proportional collection and processing is not in line with our suggestion of the co-operative model.

Both the principle of fidelity to protect the giver's free will and the principle of reasonable transactional expectation to protect the receiver's interests, which guide the requirements of an adequate consent, should be taken into account whilst looking at the relationship of trust between the two parties. First, since the fidelity principle suggests that 'every effort must be made to keep faith with the agent's will,' the relationship of trust between the two parties ought to be positive. To regard the consent giver as consenting when there is a possibility that he is actually not consenting can result in serious harm for him. To avoid this situation, the best way is

---

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)' 8. The condition of consent is set out in Article 7 of the proposed General Regulation.

[133] Beyleveld and Brownsword, *Consent in the Law* 125-227.

actually to improve the trust between the two parties. For example, seeking the giver's subjective intention to signal consent and double-checking any delayed/ unclear consent can improve the trust of the receiver. In this light, there is a lesser chance/ tendency for the consent-receiver to assume or regard the giver's lack of consent as consent. Hence, it is suggested that in relation to implementing trusted technologies, we should 'define a legal framework and describe attributes, capabilities, characteristics and qualities which allow users to verify whether the systems are trustworthy.'

Conversely, there is also a need for the receiver to believe that the giver's consent is not misleading and deceiving. With a positive relationship based on trust, the receiver may be more likely to presume that the giver's signalling of consent is reasonably trustworthy and valid.

2. Transparent Information

The co-operative model seeks to assure data subjects (consent-givers) that regardless of the application adopted, it operates according to a reliable system based on trust. Measures to ensure the easy and affordable availability of information and accurate understanding of the applications of the technology can, in effect, improve the chances for the giver to consent to the receiver's policy with respect to the applications of the technology at issue. These practices should be made accessible to all without excessive efforts and subject to independent supervision.

3. The Application of Appropriate Mechanisms

It has been suggested that data controllers, on the basis of the principle of proportionality, should 'ensure that a proper mechanism to exercise such rights is

incorporated in the application.'[134] With this in mind, PIA and PETs including choice, anonymisation and authorisation-based approaches (with their respective limitations) should be encouraged to improve opportunities for consent. To make the most of these mechanisms, however, some conditions should be noted.

First, the applications should seek to deliver the maximum degree of privacy protection by ensuring the ideas of *privacy by design* and *privacy by default*. Hence, the enhancing mechanisms of the co-operative model are better embedded into the design and architecture of applications. Secondly, it should be ascertained that such mechanisms are fully and correctly implemented.[135] Moreover, additional assessments should be taken into consideration with respect to the specificities of the data controller. For example, it is suggested that data processing in relation to biometric data requires specific attention towards the risks of identity fraud, the purpose diversion, and data breach.[136] Thirdly, it is advised that the introduction of 'an independent and legally binding control that PETs are properly implemented.'[137]

An additional mention should be made of the risks of any possible conduct resulting in unauthorised reconstruction/ re-identification/ re-link of a biometric feature to the reference template.[138] Technical measures such as the prevention of the centralised storage of biometric data and the possibility of revoking the identity link 'either in order to renew it or to permanently delete it e.g. when the consent is revoked'

[134] Article 29 Data Protection Working Party, *Opinion 3/2012 on Developments in Biometric Technologies* 9.
[135] Emilio Mordini, 'ANNEX I: Policy Brief on: Whole Body – Imaging at Airport Checkpoints: the Ethical and Policy Context' in René von Schomberg (ed), *Towards Responsible Research and Innovation in the Information and Communication Technologies and Security Technologies Fields* (Towards Responsible Research and Innovation in the Information and Communication Technologies and Security Technologies Fields 2011) 200-201.
[136] Article 29 Data Protection Working Party, *Opinion 3/2012 on Developments in Biometric Technologies* 30-31.
[137] Mordini (n 136) 168.
[138] Article 29 Data Protection Working Party, *Opinion 3/2012 on Developments in Biometric Technologies* 31.

are encouraged.[139] In this regard, the WP29 recommends the TURBINE technology which aims to 'protect the biometric template by cryptographic transformation of the fingerprint information into a non-invertible key that allows matching by bit-to-bit comparison' as well as enhancing user trust.[140]

4. Accountable Practices

In addition to technical measures for applying appropriate mechanisms, good privacy and data protection practices are also crucial in improving the relationship of trust. It has to be noted that legislative compliance is a necessary, rather than a sufficient, requirement to ensure privacy and data protection. As Solove contends that, in light of regulating privacy, technology, and security, basic principles such as minimising the collection and use of personal data and particularised suspicion rather than blanket searches should be applied.[141] In the European data protection model, for example, safety, data quality and the obligations of data controllers to provide accurate and sufficient information on the data subject can arguably improve public trust with respect to data collecting, processing and using when introducing biometric applications. It should be noted that obtaining consent *does not* absolve the obligations of the data controller under data protection practice. With such safeguards, the consent-giver is more likely to consent as their presence of consent frees up the giver from liability. Hence, the consent-giver may have reason to provide accurate personal data for the needs of scientific research and technical applications.

---

[139] Ibid 32.
[140] Ibid 32. TURBINE (TrUsted Revocable Biometric IdeNtitiEs) is an EU-funded research project elaborating a privacy-friendly biometric method with specific attention on fingerprints. For further details, see: The European Data Protection Supervisor, 'Opinion of the European Data Protection Supervisor on a research project funded by the European Union under the Seventh Framework Programme (FP7) for Research and Technology Development - Turbine (TrUsted Revocable Biometric IdeNtitiEs)' (2011) <http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2011/11-02-01_FP7_EN.pdf> accessed 23 May 2012.
[141] Solove (n 16) 172.

5. Independent Supervisory Institution

Legal regimes should be in favour of an independent authority (or more than one) to facilitate dealing with privacy and data protection issues regarding technologies at stake. Indeed, this type of regulatory design has been supported by numerous commentators. For example, Solove points out that '[g]overnment officials must be supervised to ensure that they keep their activities circumscribed, prevent abuses of power, and remain accountable for their behaviour.'[142] Moreover, with respect to the implementations of PETs, it is suggested that they create necessary public confidence towards data protection supervisory authorities (DPAs).[143] The following guidelines in relation to the roles and functions of such authority should be taken into account.

a. It is precisely due to the acceptance of the broad conception of privacy that authorities are capable of dealing with certain aspects of privacy issues *in a more efficient way*: viewed through the lens of such a broad concept, conflicts may take place and it is more appropriate to view them as conflicts between privacy values (which can be overseen by the same authority).[144]

   This is particularly important for those authorities in charge of overseeing and enforcing privacy *rights*. For example, the ICO of the UK, which is responsible for the four main fields of personal data protection and transparency of information, including the DPA, the FOIA, the Environmental Information Regulations and the Privacy and Electronic Communication Regulations, must endeavour to strike a balance between the fields they are in

[142] Ibid 172. Solove terms this the 'oversight' principle.
[143] Koorn and others (n 79) 51.
[144] It is noted that Beyleveld suggests that the conflict might also be better to be viewed as a conflict between different research values. Beyleveld, 'Data Protection and Genetics: Medical Research and the Public Good' 288.

charge of.

b. The authorities, in effect, need to play multiple roles. For example, in the European data protection model, the authority is: (1) a promoter of data protection law compliance; (2) a guardian in delivering rulings on complaints for violations of data protection laws; and (3) a defender in (assisting to) prosecuting those who are suspected of breaching data protection laws.[145] In this regard, three points have to be made:

   (1) As a promoter, public engagement should be encouraged;

   (2) As regards the roles as the guardian and the defender of privacy and data protection practice, it is considered that when the receiver and the supervisory authority is the same body or, when the supervisory authority is subject to the receiver, its trustworthiness is arguably reduced. In light of this, an *independent* body is more appropriate since the receiver can be (indeed, is usually) the government itself. Moreover,

   (3) To achieve greater performance, the authorities should be offered some margin of discretion in order to be more effective. Accordingly, they should be given the power to decide their own priorities and to start actions on their own initiative.[146]

c. The system of prior checks is better employed, or at least supervised,[147] by an independent data protection authority. This is because such data protection authority ought to possess expertise as well as public trust (due to its

[145] Section 5.2.1.2.
[146] Article 29 Data Protection Working Party, *Opinion 01/2012 on the Data Protection Reform Proposals* (No 00530/12/EN, WP191, 2012) 18.
[147] In this case, the independent data protection unit of the individual research/application project should work with the supervisory authority. Beyleveld, 'Is consent necessary and/ or sufficient to authorise medical database research?'.

independence).

d. The relationship between other authorities/ authoring bodies (such as Research Ethics Committees of biotechnological researches) and the data protection authority has to be taken into account: there is a need to distinguish the functions of each body and to reduce confusion regarding their respective functions and any existing functional overlap. This cooperation should include, for example, the legal assessment and specific supervisory measures to be taken.[148]

e. The independent privacy and data protection authority should possess necessary powers of enforcement and an adequate budget. This can improve the public trust in such authority.

We have seen that the European data protection model requires Member States to provide such an independent supervisory authority with their own jurisdiction.[149] Due to the flexibility of the Directive, the implementation of the Directive can differ in each States. However, the functions of the data protection authority should still be effectively performed. The ICO of the UK, for example, has been criticised as lacking the essential powers of enforcement (although subsequently the ICO has been awarded a substantial deterrent of a fine up to £500,000 against violations of data protection).[150]

Taiwan, however, does not adopt this approach regarding an independent data protection when borrowing from the European experience. There is, therefore, a need to analyse whether this approach can be applied generally. This will be explored in the

[148] Article 29 Data Protection Working Party, *Opinion 01/2012 on the Data Protection Reform Proposals* 19.
[149] Article 28 of the Data Protection Directive.
[150] Laurie and Sethi (n 15) 35.

following chapter.

7.4 Summary

Pragmatically, the thesis suggests that a well-designed framework can improve the relationship of trust between data subjects and data controllers in order to obtain consent. Under the co-operative model, such a framework can be seen as a safeguard with respect to both the right to benefit from advances in science and technology and privacy and data protection rights. In this regard, an *independent* supervisory authority can possess the characteristics of expertise, transparency, efficiency and due process – based on trust towards public authorities. Indeed, by establishing a trustworthy institutional framework, although reconciling competing values of regulatory design can be difficult, those values are capable of presenting positive-sum outcomes.

Chapter 8

A PGC-compliant Regulatory Framework and Rule of Personal Data Protection for Taiwan

8.1 Introduction

As we have seen in Chapter 5, there are limited specific regulations in Europe as well as in Taiwan that govern rapidly developing technologies considered here. At the beginning of this chapter, I will analytically compare the regulatory positions of Europe and Taiwan for the relevant technology. This inquiry will focus on privacy and personal data protection issues. It is observed that the objectives and principles of data protection are similar in both areas, as the Formosan data protection regime borrowed a number of practices from the European data protection model. However, some differences between the two regimes exist. To discuss this, the chapter will cover three themes among the differences, namely consent and public interests, the operation of data protection principles in practice, and the relevant supervisory authorities. Situations will be identified as being consistent or not with the requirements of the PGC. I argue that such regulatory mechanisms must be critically justified on the basis of the PGC.

On the basis of the analysis, this chapter aims to propose a PGC-derived regulatory framework and rule of personal data protection with respect to development of technology for Taiwan. The regulation of both data protection regimes is suboptimal and thus can be improved. Lessons for Taiwan may be learned from the

European data protection model experience and vice versa.

8.2 The Analytic Comparison of Regulation between Taiwan and Europe: Biometric and RFID Technologies

This comparative section will analyse the provisions of the European and Formosan privacy regime in a sense of *microcomparison*[1] concentrating on specific legal problems in relation to biometric and RFID technologies. Two elements of comparative methodology are necessarily involved, namely the exploring of both similarities and differences. This is because, as Dannemann observes, that 'there is no point in comparing what is identical, and little point in comparing what has nothing in common.'[2]

On the one hand, based on the functional-approach[3] towards microcomparison, it can be presumed that different legal regimes may express similar solutions to similar cases. On the other hand, other scholarly writings tend to consider the difference theory. This is because comparative study highlights contrasts; therefore differences constitute the first and foremost phenomena to observe.[4] Additionally, critics of the functionalists argue that the focus of functionalism on result-based comparisons

[1] The comparative studies which focus on general question are termed by Zweigert and Kötz as the macrocomparison. On the other hand, those focuses on specific legal problems are termed as the microcomparison. See: Konrad Zweigert and Hein Kötz, *An Introduction to Comparative Law* (Tony Weir tr, 3rd edn, OUP 1998) 63. Also, Gerhard Dannemann, 'Comparative Law: Study of Similarities or Differences?' in Mathias Reimann and Reinhard Zimmermann (eds), *The Oxford Handbook of Comparative Law* (OUP 2006) 387-388.
[2] Dannemann (n 1) 384.
[3] The functional method puts great emphasis on distinguishing differences within similarity. For further discussion, see: Ralf Michaels, 'The Functional Method of Comparative Law' in Mathias Reimann and Reinhard Zimmermann (eds), *The Oxford Handbook of Comparative Law* (OUP 2006) 339-382. Also, Dannemann (n 1) 388.
[4] Dannemann (n 1) 387.

should be avoided.[5]

However, it is worth noting that, as Jansen puts, 'comprehensive comparative knowledge requires an analysis both of similarities and dissimilarities, and of genetic relations, for they complement each other.' [6] In this regard, the comparative judgements of this section will take the PGC as the *tertium comparationis*[7] relating to observable explanatory similarities and dissimilarities. The first subsection will focus on the similarities of the two legal regimes, and the remaining subsections will specifically discuss the analytic dissimilarities which will require emphases on different regulatory methods and responses.

8.2.1 Not So Different: the Framework of Legal Protection

As a preliminary matter, it should be noted that both Taiwan's academic lawyers and policymakers have adopted elements of western jurisprudence, particularly the German system. The result of this is a rather complex hybrid legal regime.[8] Under no circumstance is the assessment of the fluid nature of the right to privacy in Taiwan able to avoid these systemic complexities.

The European countries and Taiwan share a high level of similar protection of personal data by having a main regulatory provision. In the EU it is the Data

[5] Ibid 390.
[6] Nils Jansen, 'Comparative Law and Comparative Knowledge' in Mathias Reimann and Reinhard Zimmermann (eds), *The Oxford Handbook of Comparative Law* (OUP 2006) 337.
[7] *Tertium comparationis* is the quality that two things which are being compared have in common. Jansen regards this as a choice about 'what matters' in relations aspects 'of the law are relevant for the comparative lawyer, and which aspects of the law might benefit from the additional knowledge which comparison provides.' Ibid 314-315.
[8] Chung-Lin Chen, 'In Search of a New Approach of Information Privacy Judicial Review: Interpreting No. 603 of Taiwan's Constitutional Court as a Guide' (2010) 20 Indiana International and Comparative Law Review 27.

Protection Directive. As regards the main data protection regulatory instrument in Taiwan, since the PDPL (as well as the CPDPL) is profoundly influenced by the European model, it is inevitable that they share a great number of common regulatory methods. For example, the main legal protection bases both aim to protect fundamental rights and freedoms of individuals/ the right to personality, and in particular their right to privacy with respect to the collection, processing and use of personal data.

1. Personal biometric data is treated as sensitive personal data. How about the biometric samples?

Neither the Data Protection Directive nor the PDPL specifically mention biometric data. However, as was discussed in the previous chapter,[9] it is arguable that the Directive covers biometric data as far as the data subject concerned is able to be identified or identifiable.[10] Moreover, biometric data can be considered as sensitive data since it could reveal, or openly include, either health data, data on ethnic origin, or sexual life, e.g., homosexuality,[11] – if there is a possibility to reasonably *identify* or *relink* biometric data and relevant sensitive data.

With respect to the Formosan data protection regime, on the other hand, biometric data can also fall under the categories of sensitive data since it is related to either genetic information or sex life. For example, fingerprints have been regarded as a type of sensitive data by the Honourable Justices:

---

[9] Section 2.3.1.2.
[10] See Chapter 7. For a similar argument particularly in relation to DNA and the genetic data, see: Ségolène Rouillé-Mirza and Jessica Wright, 'Comparative Study on the Implementation and Effect of Directive 95/46/EC on Data Protection in Europe: Medical Research' in Deryck Beyleveld and others (eds), *Data Protection Directive and Medicial Research Across Europe* (Ashgete Publishing 2004) 193-194.
[11] J. A. Y. Hall and D. Kimura, 'Dermatoglyphic Asymmetry and Sexual Orientation in Men' (1994) 108 Behavioral Neuroscience 1203.

> Fingerprints are biological features of an individual's person, which are characterized by personal uniqueness and lifetime unchangeability. As such, they will become a form of personal information that is highly capable of performing the function of identity verification once they are connected with one's identity. Because fingerprints possess such trait as leaving traces at touching an object, they will be in a key position to opening the complete file of a person by means of cross-checking the fingerprints stored in the database. As fingerprints are of the aforesaid characteristics, they may very well be used to monitor an individual's *sensitive* information if the State collects fingerprints and establishes databases by means of identity confirmation. (emphasis added)[12]

Yet this viewpoint was not totally appreciated by every Honourable Justice (nor the government). In the dissenting opinion held by (the former) Honourable Justice Syue-Ming Yu, for example, it is argued that, by citing two U.S. cases,[13] although the fingerprints themselves are a type of personal information (data), they may not necessarily involve the violation of the right to privacy. This is because: (1) fingerprints do not fall within the scope of 'physical condition' thus they cannot be viewed as 'the medical information' that 'the Legislature regarded as too private to be made available to the public';[14] and (2) the right to privacy regarding fingerprints is without substance since '[t]he day is long past when fingerprinting carried with it a stigma of criminality.'[15] Nevertheless, such arguments can no longer stand after the amendment of the CPDPL.

---

[12] J. Y. Interpretation No. 603.
[13] See Judge Mosk's dissenting opinion in *Thomas v. New York Stock Exchange*, 306 F.Supp. 1002 (S.D.N.Y. 1969) and *Perkey v. Department of Motor Vehicles* (1986) 42 Cal.3d 185, 228 Cal.Rptr. 169; 721 P.2d 50. He also considered that 'a fingerprint is merely an additional means of identifying the applicant, like age, sex, weight, height, hair and eye colour -- all of which, I note, this petitioner is perfectly willing to reveal.'
[14] *Perkey v. Department of Motor Vehicles* (1986) 42 Cal.3d 185, 228 Cal.Rptr. 169; 721 P.2d 50.
[15] *Thomas v. New York Stock Exchange*, 306 F.Supp. 1007 (S.D.N.Y. 1969).

A further question is whether the biometric *samples* could be considered as sensitive data. DNA samples, for instance, have not been regulated in the Data Protection Directive and the related guidance. It is observed that '[v]ery often the situation in the individual country is unclear in relation to either genetic information or samples.'[16] In the Formosan context, similarly, the PDPL refers to genetic and sex life information within the scope of sensitive data. Yet it remains unclear with respect to samples themselves. Nevertheless, it is worth noting that Article 18 of the Human Biobank Management Act[17] provides:

> (I) Any storage, use, or disclosure of the concerned operator's entire biological *specimens* and related data and information shall be encoded, encrypted, delinked, or transformed so that the participant's identity is unable to be determined.
>
> (II) An Operator shall encrypt and independently administer information that can determine the identity of an individual participant, such as his/her name, identification number, and date of birth. An Operator shall establish a review and control procedure for cross referencing the aforesaid personal information with the biological *specimens* and relevant data and information. Such information shall be restored immediately after each necessary use…

Although the purpose of this Act specifically refers to *medical research on biometrics*,[18] e.g. genes, to reason by analogy form this legal provision, it is arguable (and seems to me to be convincing) to suggest that biometric samples *for any*

[16] Rouillé-Mirza and Wright (n 10) 194.
[17] Available at< http://law.moj.gov.tw/Eng/LawClass/LawAll.aspx?PCode=L0020164>, accessed 14 May 2011.
[18] Article 3(4) states that the term 'biobank' refers to 'for the purpose of biomedical research, the Biobank contains participants' biological specimens, natural persons' information and other related data and information based on human population or specific groups. These biological specimens, derivatives, or relevant data are stored in the 'biomedical research.' And the term 'biomedical research' is defined by Article 3(3) as referring to 'medical research on basic *biometrics*, such as genes.' (emphasis added)

purposes should fall under the sensitive data protection regime. This is because there appears, furthermore, to be no reason in principle why the notion of 'sensitive data' should be taken to exclude any other purpose.

2. Similar data protection principles

It has been suggested by the WP29 (of the EU) and the T-PD (of the CoE) that a number of basic data protection principles, e.g., the principle of purpose specification, the principle of proportionality, and the principle of precautionary,[19] have to be taken into account when processing biometric data.

Reflecting the greatly influential European model, the PDPL also covers a number of general data protection principles. As regards biometric data, it is stated by the Human Biobank Management Act in its Article 20 that '[a]ny use of biological specimens, derivatives and relevant data and information in the Biobank shall not be used for purposes other than biomedical research.'

However, such principles are inevitably followed by a number of exceptions. A more detailed comparison between the European and Formosan provisions will be provided in the next subsection, focusing on the differences.

Overall, looking micro-comparatively at the developing technologies at hand, the Formosan regulatory tools are similar to the European ones. However, it is referred by the Constitutional Court that '[d]espite the admissibility of other nations' similar

[19] Working Document on biometrics, 1 August 2003, available at: < http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2003/wp80_en.pdf >, accessed 14 May 2011. The Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, 'Progress Report on the Application of the Principles of Convention 108 to the Collection and Processing of Biometric Data' (*T-PD*, 2005) <http://www.coe.int/t/e/legal_affairs/legal_co-operation/data_protection/documents/reports_and_studies_of_data_protection_committees/2Biometrics_2005_en.pdf> accessed 13 February 2010.

legislations and domestic popular polls as materials used in interpreting the Constitution, they cannot be used as the sole basis of determining the meanings and intents thereof.'[20] This is particularly true in terms of the complex hybrid Taiwanese legal regime. It is thus unsurprising to find that some local commentators may criticise the fact that the European model of regulating personal data is impractical due to the rigid approach of seeking maximum privacy protections, which can become a barrier to the free flow of information.[21] Many local commentators thus hold the opinion that the European model may not be suitable for Taiwan.

However, I argue that there is a need to re-affirm the European model in the Formosan data protection regime.[22] This is because:

a. Although the European model has set a high standard for protecting the right to (informational) privacy, this is not prohibited by the PGC since such a right is a generic right. On the contrary, it is welcomed.
b. It must not be forgotten that one of the purposes of the Data Protection Directive is to *improve the information flow*. Moreover, the proposal of the EU General Data Protection Regulation clearly addressed that '[t]his Regulation lays down rules relating to the protection of individuals with regard to the processing of personal data and rules relating to the free movement of personal data.'[23] Indeed, the improvement of the information flow and privacy are two sides of the same coin. Therefore, there seems to be

[20] J. Y. Interpretation No. 603.
[21] Ming-Li Wang, 'Information Privacy in a Network Society: Decision Making Amidst Constant Change' (2010) 5 National Taiwan University Law Review131-136.
[22] See also: Directorate-General Justice European Commission, Freedom and Security,, 'Comparative Study on Different Approaches to New Privacy Challenges, in Particular in the Light of Technological Developments' (2010) <http://ec.europa.eu/justice/policies/privacy/docs/studies/new_privacy_challenges/final_report_en.pdf> accessed 30 Janurary 2012, para. 27.
[23] Article 1(1).

a misunderstanding behind the objection to the Directive on the grounds that it places greater emphasis on the protection of personal data rather than the free flow of information. Meanwhile, the WP29 addresses that the interpretation should not be 'unduly restricted' or 'overstretched.'[24] With this in mind, in Article 1(3) of the proposal of 2012 EU General Data Protection Regulation, it is stated that '[t]he free movement of personal data within the Union shall neither be restricted nor prohibited for reasons connected with the protection of individuals with regard to the processing of personal data.'

c. The benefits of this right can be waived by valid consent under the will-conception (which is, as argued in Chapter 5, in line with the European data protection model), thus there is not a necessary conflict between the rights and interests; and

d. When there is actually a conflict between values regarding advances of science and technology and privacy and data protection values, without a valid consent, there is a violation of the right to privacy and the right to data protection unless there is a substantive justification on the basis of the criterion of degrees of needfulness of generic conditions of agency. Moreover, on the basis of previous discussion of the co-operative model, the right to privacy under the European model is not necessarily a barrier to the other rights.

8.2.2 Not So Similar (I): Consent and Public Interests

It has been emphasised that consent as a procedural justification is crucial to data

[24] Article 29 Data Protection Working Party, *Opinion 4/2007 on the Concept of Personal Data* (No 01248/07/EN, WP136, 2007) 5-6.

protection and privacy questions. Both data protection regimes carry a number of consent elements. However, the status of consent is implicitly stated in both regimes. It thus seems that the role of consent is quite similar in the context of both regimes.

Nevertheless, this is not quite the right understanding. With respect to the European perspective, it has been demonstrated that although the Data Protection Directive does not clearly emphasise the principle of priority of consent, one should not invite interpretations departing from this principle.[25] In the *M. S. v Sweden* case which is in agreement with the criterion in terms of will-conception thinking,[26] for example, it has been held by the ECtHR that processing sensitive personal data without consent violates the right to private life under Article 8 of the ECHR.[27]

On the other hand, however, this may not be valid in Taiwan. As pointed out previously, there is confusion around the validity of consent under the PDPL: there is an absence, whether intentional or not, of the issue of consent in the sensitive data rules (Article 6 of the PDPL). Moreover, in J. Y. Interpretation No. 603, the principle of priority of consent when processing sensitive personal data has not been mentioned. An alternative argument, therefore, is needed. To meet this need, I have argued that, based on the Gewirthian moral principles, Article 6 of the PDPL requires, at least implicitly, a practicable consent as an exemption to the barring of processing and collecting sensitive data. Nevertheless, the question of 'why does the (Formosan) law not address the obtaining of consent as an exemption when processing sensitive categories of personal data' still needs to be analysed in greater detail when discussing

[25] See Chapter 5.
[26] *MS v Sweden* (1999) 28 EHRR 313, paras 34-35. See also, section 4.3.2 and *Z. v Finland* (1998) 25 EHRR 371.
[27] Deryck Beyleveld, 'An Overview of Directive 95/46/EC in Relation to Medical Research' in Deryck Beyleveld and others (eds), *The Data Protection Directive and Medicial Research Across Europe* (Ashgate Publishing 2004) 11.

the regulation method.

By acknowledging the confusion of the issue of consent in the PDPL framework, it seems that Formosan law makers do not *sincerely* follow the aim of the PDPL to prevent the *harm of the right to personality* – at least not as sincere as their European accompany. A handful of observations in relation to the PDPL reflect this:

1. There is no consent exemption in Article 6 of the PDPL. It might invite a misunderstanding that even though a data subject gives her valid consent, no one can collect or process her sensitive personal data unless at least one of the exemptions in Article 6 (e.g., in accordance with law, the fulfilment of the legal obligation) is engaged.[28] In effect, this misunderstanding may be occurred in judicial reviews if the court strictly follows the wording of the PDPL.
2. Although 'nothing in the Data Protection Directive states clearly that any condition takes priority over by another,'[29] consent is the leading condition in Articles 7 and 8. Indeed, what really matters is the reason why consent as a procedural justification is key. With respect to Article 8(1) of the ECHR, for example, the violation of the rights granted is engaged without a valid consent, unless Article 8(2) is justified. Nevertheless, this is not the case in the PDPL in terms of sensitive personal data, which should be protected at a higher level.[30]
3. Lastly, it is worth noting that the first condition in these four articles (in relation to the conditions for the principle of purpose) is the same: to fulfil the

[28] Section 6.4.1.
[29] Beyleveld (n 27) 11.
[30] As regards non-sensitive personal data, the consent condition in play is the second and the fifth in Articles 15 and 19 respectively, let alone it is the *last* condition in Articles 16 and 20.

functions provided in the laws and regulations. With regard to the exemptions from the prohibition on collecting and processing sensitive personal data (e.g. biometric data), unsurprisingly, the fulfilment of the legal obligations is on the top of the list in Article 6 of the PDPL.

Therefore, the observations set out above seem to imply that the Formosan regulation method gives extra weight to collective interests (the value of obeying the law) rather than the individual interests and their choices.[31] On the basis of this, it can accordingly be argued that the Formosan hybrid legal regime is still significantly influenced by the traditional Chinese value of 'sacrificing the "small" me, for the completion of the "big" me,' i.e., **sacrificing oneself for the sake of the whole**.

How to look at this problem on the basis of the PGC?

The generic rights of an agent balance (according to the criterion of degrees of needfulness for action) vis-à-vis other rights – generic rights of other agents, either individually or *collectively* as the State/ community. Since law has its own culture of relative restraint,[32] the way that consent is managed can be different. Nevertheless, it should always be borne in mind that, under Gewirthian theory, the rules governing interactions between agents in a complex community should not be confused with the rationale upheld by Utilitarianism. Specifically, it is not a regulative method trying to maximise utility for a State as a whole regardless of the cost borne by some of its members (i.e., data subjects who provide biometric data). Instead, 'it is that of imposing relatively slight costs on some persons only in order to prevent far greater

[31] It is noted that the English courts have tended to interpret the scope of public interest in rather 'broad and inconclusive terms.' However, the courts, in the particular situations of each case, still balance privacy and competing public interest. See: Deryck Beyleveld and Shaun D. Pattinson, 'Confidentiality and Data Protection' in Andrew Grubb, Judith Laing and Jean McHale (eds), *Principles of Medical Law* (3rd edn, OUP 2010) 666.
[32] Deryck Beyleveld and Roger Brownsword, *Consent in the Law* (Hart Publishing 2007) 334.

costs from having to be borne by other persons, so that an equality of generic rights for all persons may be more nearly approached.'[33] This is particularly crucial when looking at sensitive personal data, which contains information for accessing the complete files of data subjects. It has been suggested that 'where a society takes individuals and their consent seriously – particularly so, perhaps, where social relationships are framed by a respect for human rights – the concept of consent will come to play a key role in its practical thinking.'[34]

In the Formosan data protection regime, although there is confusion on the validity of the consent element, there is no denying that consent does play a role in the PDPL. Recently, the awareness of the importance of individual rights and related voluntarily choices has been reflected in Taiwan's data protection regime. In terms of the accessing biometric data, for example, the growing awareness of the principle of priority of consent is reflected to in Article 6(I) of the Human Biobank Management Act:

> Collections of biological specimens shall be conducted in compliance with medical and research ethics. Participants shall be informed of related matters in a clearly comprehensible manner. Such matters shall be specified in an agreement of consent. Any collection may only be undertaken after the participant's written consent is obtained.

8.2.3 Not So Similar (II): the Operation of Data Protection Principles

This subsection will focus on how the data protection principles operate in the

[33] Alan Gewirth, *Reason and Morality* (University of Chicago Press 1978) 344.
[34] Beyleveld and Brownsword, *Consent in the Law* (n 32) 2-3.

European and Formosan regimes. For regulators it is easy to realise that, as cited by Brownsword in referencing UNESCO,[35] there is a need for the establishment and the maintenance of regulatory regimes to enable individuals to enjoy the benefits of science and technology and ensure that fundamental human rights and freedoms are fully respected and protected. It is, however, never going to be easy to put this into practice – either in the European or the Formosan legal regime. It has been contended in the opening chapter that the primary hurdle to biometric and RFID technologies is the data protection concerns, e.g., function creep, data tracking, and data profiling. To deal with such concerns, a number of data protection principles, as well as the advantages promised and the right to the benefits of these technologies, need to be taken into account.

Let us start from the purpose principle, which is particularly helpful to deal with the function creep and data profiling problems brought about by the RFID applications. In Europe, the main data protection regulatory instrument declares that personal data must be '…collected for specified, explicit, and legitimate purposes and not further processed in a way *incompatible* with those purposes.'[36] The Directive itself does not provide clear guidance on the exact meaning of 'incompatible' processing. In an investigation in relation to the European data protection law regime, it has been pointed out that although most of the Member States follow the term 'incompatible', some countries (e.g. Germany, Greece, the Czech Republic, and Latvia) go further by stating that 'the data may only be further processed for the purpose for which they were originally collected.'[37] For example, the (German) Federal Data Protection Act (Bundesdatenschutzgesetz, BDSG, 1 September 2009)

[35] Roger Brownsword, *Rights, Regulation, and the Technological Revolution* (OUP 2008) 284.
[36] Article 6(b) of the Data Protection Directive.
[37] Rouillé-Mirza and Wright (n 10) 208.

states in its Section 14(1):[38]

> The recording, alteration or use of personal data shall be lawful when required to carry out the tasks for which the controller is responsible and *for the purpose for which the data were collected*. If no prior collection took place, the data may be altered or used *only for the purpose for which they were recorded*. (emphasis added)

By virtue of such provision, this approach accordingly presents some exceptions.[39] As a legal regime adopting transplants mainly from the German experience, Taiwan follows this approach in Articles 19 and 20 of the PDPL.

Yet two dissimilarities are worth noting when considering the different regulatory methods. These two differences are termed '**the two worships**' here. The first one is the **worship of public interest**, which has already been discussed with respect to the consent issues in the last subsection. In the German implementation of the Directive, the exemption requires to 'prevent significant disadvantages to the common good or a threat to public security or to preserve significant concerns of the common good.'[40] Although it does not clearly mention that the common good must override the rights of the data subjects, the requirement of 'significance' does imply a similar requirement. The proportionality principle should be taken into account in this regard. However, in the PDPL, the public sectors is allowed to justify the violation of the purpose principle wherever the 'public interest is involved.'[41]

---

[38] This English translation is accessed from the official website of the (German) Federal Commissioner for Data Protection and Freedom of Information. Available at < http://www.bfdi.bund.de/EN/DataProtectionActs/Artikel/BDSG_idFv01092009.pdf?__blob=publicationFile > accessed 21 May 2011.

[39] There are 9 conditions of lawfully recording, alteration or use for other purposes in Section 14(2) of the BDSG. There conditions can be viewed as the exemptions of Section 14(1).

[40] Section 14(2)6 of the BDSG.

[41] To interpret this, it is plausible to apply the balancing tests such as the proportionality principle. However, the justification of using the test may be weaker, as the text of the article mentions only the

It should be noted that the proposal of the EU Data Protection Regulation has introduced broad exceptions for public authorities on the grounds of public interest.[42] If this is the trend, then this is similar to the Formosan worship of public interest. However, the WP29 criticises this approach as such broad and unspecified exceptions, which lack 'adequate safeguards for the protection of individuals,' are unjustified.[43] With this in mind, in contrast to the Formosan worship of public interest, which offers an extremely broad exception of 'wherever the public interest is involved,' the WP29 suggests the proposed Regulation should identify the specific public interests in as much detail as possible.[44]

The second worship is the **worship of research**. It is frequent; sometimes even essential, to use biometric data for scientific/ biotechnological/ academic/ medical research. The German exemption for reasons of scientific research is described as

> …*necessary* for the purposes of scientific research, where the scientific interest in carrying out the research project *significantly outweighs* the data subject's interest in ruling out the possibility of collection and the purpose of the research cannot be achieved in any other way or would require a *disproportionate* effort. (emphasis added)[45]

Moreover, when using sensitive data for scientific research, the BDSG provides in Section 14(5):

> In weighing the public interest under the first sentence, no. 2, *special attention shall*

---

involvement of public interest.
[42] E.g., Articles 6(4), 9(2)(g), 17(5), 21(1)(c), and 33(5) of the proposed General Regulation.
[43] Article 29 Data Protection Working Party, *Opinion 01/2012 on the Data Protection Reform Proposals* (No 00530/12/EN, WP191, 2012) 12-13.
[44] Ibid 12.
[45] Section 14(2)9 of the BDSG.

be paid to the scientific interest in the research project.

(emphasis added)

On the other hand, the PDPL has a considerably lenient standard in relation to the purpose principle (as well as other principles such as the principle of proportionality). It simply states that where it is necessary in the name of *public interest* for the purpose of academic research conducted by an official research institution, and as long as the personal data '*may not* lead to the identification of a certain person after the treatment of the provider or the disclosure of the collector,' the data controllers can further process personal data beyond the original purpose.[46]

This 'generous offer' for academic research has been criticised by the local commentators as it comprehensively reduces the burden of respecting data protection principles such as the purpose principle.[47] Furthermore, such a regulatory operation also calls attention to the potential violations of the right to personality since the consent justification is not even mentioned in Article 6 of the PDPL.

It seems plausible to regard the benefits of research as falling under the scope of 'the economic-social rights' defined by the ICESCR, and relate the right to privacy and personal data protection to 'the political-civil rights' embodied in the ICCPR. This is because while Article 17 of the ICCPR mentions the right to privacy, Article 15(1)(b) grants a right to benefit from advances in science and technology. In this regard, the 'full-belly' thesis contends that, in terms of the two separate sets of rights,

[46] Articles 19 and 20 of the PDPL.
[47] Ching-Yi Liu, 'Not So Improved: Initial Commentry on the Personal Data Protection Law' (2010) 183 The Taiwan Law Review152-156. Also, Wen-Tsong Chiou, 'Comments on the Framework Problems of the Draft of Computer-Processed Personal Data Protection Law from the Perspective of the Conceptual Distinction between Information Self-determination and Information Privacy' (2009) 168 The Taiwan Law Review 184-186.

the economic-social rights should take priority over the other set of rights.[48] This is because it is implied, on the basis of the 'full-belly' thesis, that economic rights to subsistence are 'basic needs' which should be fulfilled before an individual can 'indulge in the "luxury" of worrying about her political freedoms.'[49]

Does such a worship of the 'research privilege' in Taiwan's data protection regime support the disputed interpretation that economic-social rights are more crucial than political-civil rights? Will such a research interest which might be able to save lives, prevent from illness, or extend life spans, be considered as being more needed for agency than other objects of the political-civil rights? Three points must be made to respond to this, with reference to the criterion of degrees of needfulness for action.

1. The PGC does not deny that there is a right to benefit from research, since such research protects or improves *generic rights* such as life, health or a more comfortable life. Such a right can be considered at least as an additive right since in many cases the benefits of research can improve an agent's capacities for successful action, regardless of the agent's purposes.[50]
2. The PGC does not presume that economic-social rights should outweigh political-civil rights, or vice versa.[51] Gewirth himself disproves the thesis arguing that economic-social rights should outweigh political-civil rights (for example, the generic need for food is prior to the civil liberties) by offering three reasons:[52]

[48] Rhoda Howard, 'The Full-Belly Thesis: Should Economic Rights Take Priority over Civil and Political Rights? Evidence from Sub-Saharan Africa' (1983) 5 Human Rights Quarterly 467-490.
[49] Ibid 469. Also, Alan Gewirth, *The Community of Rights* (The University of Chicago Press 1996) 53.
[50] See section 6.2.
[51] In Howard's article, similarly, he contends that he is not saying that 'civil and political rights must take priority over economic, social, and cultural rights.' This is because, as he argues, that the two sets of rights are 'interactive, not sequential.' See: Howard (n 48) 469.
[52] Gewirth, *The Community of Rights* 53.

a) Some violations of political-civil rights (such as torture and summary execution) can be as serious as some violations of economic-social rights (such as the prevention of being in a state of starvation).
b) The requirement of equal distribution of political-civil rights can control the distribution of economic-social rights via the determination of political power in a community.
c) Political-civil rights are essential for equal human dignity which is consistently required by the PGC.

In fact, each *group* of rights (political-civil rights and economic-social rights) contains different *categories* of generic rights (i.e., the basic rights, non-subtractive rights, and additive rights) within the hierarchy criterion. Moreover, the generic rights within the same category of needs are also placed in a hierarchical order. Without being specific on which right is at issue, one is unable to identify which objects should be compared based on this criterion.[53] In other words, we should not forget that which generic rights can override the other can only be decided on a case-by-case basis.

3. It appears that the full-belly argument is in agreement with the conflict model in relation to a narrow conception of privacy. These two categories of rights, however, are not necessarily in conflict. The PGC requires the prevention of violating generic rights rather than increasing the amounts of goods. Without the infringements of generic rights, the criterion of degrees of needfulness for action simply does not come into play. With this in mind, we must not forget that the improvement of the benefits and interests of economic rights is *also* an improvement of the right to private life. In other words, this right can be

[53] See section 4.3.4.

both political and economic in nature. Moreover, indeed, with respect to the three reasons given above which disprove the full-belly thesis, the co-operative model can be used to identify what is wrong with this thesis: the two sets of rights in play are simply not always a game of zero-sum trade off.

Let us take an example which is adduced in Gewirth's remark: 'since driving automobiles, which may lead to deaths, is less needed for action than is life, the criterion (of degrees of needfulness for action) might be held to justify infringing the right to drive automobiles.'[54] Gewirth responses this thesis by arguing:[55]

> Person's freedom of action normally involves that they can control how they drive and hence their degree of risk in driving. The driver can markedly lower this risk by driving carefully and defensively and by abstaining from liquor and drugs. Since it is the driver who mainly *controls whether and to what extent her life will be endangered*, she is still *enabled to give primary weight to the right to life*, despite the statistical possibility of mortal accidents. Thus the hierarchic priority of the right to life over the right to drive automobiles, which reflects the criterion of degrees of needfulness for action, is not refuted by the lethal possibilities of the latter right. (emphasis added)

In this case, what Gewirth does not clearly point out is that, by considering the voluntarily choice (which can control/ decide whether, and to what extent, to waive the benefits of an agent's generic rights) as able to play a part in the reconciliation between two kinds of rights, there is not necessarily a conflict. Since the conflict has not occurred, the criterion is, by its own nature, not

[54] Gewirth, *The Community of Rights* 50.
[55] Ibid 54.

refuted. In the above case it is the ability to control whether and to what extent the agent's life will be endangered that prevents/ diminishes the two above-mentioned rights from coming into conflict.

Overall, the generic conditions of agency cannot be culturally or legally dependent since there are no such binding requirements outside the context of the PGC. Hence, no matter which regulatory method is chosen to reflect the legal culture, the primary task should be the genuine attempt to avoid conflict between generic interests. This can be achieved by introducing the co-operative model. If conflicts cannot be prevented, then the criterion of degrees of needfulness for action should be applied. Therefore, if the 'worship of research' model fails to strike a balance between the right to benefit from research and the other fundamental rights and freedoms in relation to processing personal data, then the former right has to be considered based on the criterion provided by the PGC.

8.2.4 Not So Similar (III): The Supervisory Authorities

The independent supervisory authority (or authorities) has been indicated in the Directive as the main safeguard on data protection in Europe. It has been suggested that the national supervisory authority in each Member State plays multi-functional role as the promoter, the guardian, and the defender of the data protection. Some regulatory safeguards in the Directive such as prior checking of processing operations (Article 20) and notification (Article 18) are essentially related to such authorities. To be more specific on the processing of biometric data at the domestic level, for example, several European countries require that processing biometric data for the

health purposes must be checked or authorised by an Ethics Committee and supervisory authority.[56]

However, the Formosan data protection regime is quite different from the European model in this regard – there is no supervisory authority responsible for the application of the PDPL. Article 25 of the PDPL simply states that

> [f]or the non-government agency that violates the provisions of this Law, one of the following actions may be ordered jointly with a fine *as regulated by the government authority in charge of subject industry* at the central government level, municipality directly under the central government, or county or city government…

This evokes radically divergent views.

Perhaps the most common characteristic shared by the data protection regimes worldwide is that there is always a gap between the law and the explosive growth of technology. This problem might be tackled to some extent by the government authorities themselves rather than an 'outsider,' since those authorities are: (1) usually more professional to specific techniques than those law makers in general; and (2) easier to make quick and targeted responses.[57] Accordingly, it might be argued that the Formosan model is easier to manage and to adapt to data protection concerns in connection with specific technologies. For example, it less likely for law experts in the Ministry of Justice to be aware of the possibility of function creep problem in the private field, yet the scientific experts under the Ministry of the Economic Affairs may identify and deal with these issues more easily.

[56] Rouillé-Mirza and Wright (n 10) 222-223.
[57] Wang (n 21) 146, cited from Richard Stewart, 'Reformation of American Administrative Law' (1975) 88 Harvard Law Review 1669.

However, what appeared in the first reading of such a flexible management model in Taiwan has emerged as a tangled set of experiences that reflected quite the opposite to what was expected. As might be easily assumed, public agencies have adopted quite different strategies to meet the CPDPL requirements and have developed diverse interpretations and decisions in relation to similar cases. For example, for public officials in scientific capacity, the worship of the 'research privilege' cannot be totally avoided. In contrast, the authorities regulating the media and press may try to be more favourable towards privacy concerns (or any other competing interests such as protection of minors) on the basis of trends towards higher supervision. This thus commits a hydra-headed bureaucracy problem. Based on the inefficient and problematic experiences of the CPDPL and considering the integrity of the whole data protection framework, Taiwanese scholars suggest that the law-makers should follow the European approach to establish a supervisory authority to supervise this area.[58]

8.3 Next Steps for Taiwan: A PGC-compliant Regulatory Framework and Rule of Personal Data Protection

Now that we know the similarities and differences between the two data protection regimes, we are able to turn our attention to the content of a PGC-derived regulatory framework governing biometric and RFID technologies for Taiwan. It is recalled that the European data protection model roughly matches the PGC requirements, whilst being unaware of the PGC as the supreme moral principle. Even some regulatory approaches, arguably, may be considered as not fitting neatly with the requirements of the PGC, though at least they are not expressly forbidden by the supreme principle of

[58] However, this is not accepted by the legislators when amending the law.

morality. The European data protection model has profoundly influenced global data protection laws including the Formosan regime; in what areas has Taiwan learned from that model? This will be discussed on the basis of the guidelines provided in the previous chapter. Moreover, a number of best practices suggested by reports of the Scottish Health Informatics Programme[59]as well as opinions adopted by the WP29[60] are taken into consideration and re-structured on the PGC basis.

8.3.1 Regulatory Attempts (I): Applying the Co-operative Model to the Regulations and Their Interpretations

It has been argued that the co-operative model is more effective if efficiently applied. The keys of the success of this model depend on the elements which are worth revisiting, listed below:

1. The Acceptance of A Broad Concept of Privacy

It has been emphasised that the acceptance of a broad conception of privacy is of central importance with regard to the practical application of the co-operative model. It is arguable that, however, the European expansionist approach may result in comprising everything. For example, section 3(1) of the BDSG refers personal data to

[59] E.g. Graeme Laurie and Nayha Sethi, 'Information Governance of Use of Patient Data in Medical Research in Scotland: Current and Future Scenarios' (*Scottish Health Informatics Programme (SHIP)*) <http://www.scot-ship.ac.uk/sites/default/files/Reports/Scoping_Report_Final_August_2010.pdf> accessed 6 August 2011 and Scottish Health Informatics Programme (SHIP), 'SHIP Guiding Principles and Best Practices: A document of the SHIP Information Governance Working Group' (*Scottish Health Informatics Programme (SHIP)*, 22 October 2010) <http://www.scot-ship.ac.uk/sites/default/files/Reports/Guiding_Principles_and_Best_Practices_221010.pdf> accessed 17 October 2011.

[60] E.g., Article 29 Data Protection Working Party, *Opinion 3/2012 on Developments in Biometric Technologies* (No 00720/12/EN, WP193, 2012) and Article 29 Data Protection Working Party, *Opinion 9/2011 on the Revised Industry Proposal for a Privacy and Data Protection Impact Assessment Framework for RFID Applications* (No 00327/11/EN, WP180, 2011).

'any information concerning the personal or material circumstances of an identified or identifiable natural person.' Such a broad concept may be viewed as being too broad to deal with different levels of data protection. This might lead to a conviction that the two types of data should be treated as equivalent categories.[61] However, this is not so true. Taking section 3(1) of the BDSG as an example, a broad conception of privacy does not require agents/ regulators to treat the two categories (i.e., the identified and identifiable agent) equally; rather, it simply ask regulators to treat them within the concept of privacy. It is recalled that under the PGC line of reasoning, different generic needs are ordered in a hierarchy and within the same level of generic needs, although there is still a hierarchy of generic needs since the degree of needfulness for action are different.[62] In other words, to consider both categorises as conceptions of privacy does not necessarily mean that they will be treated them equally.

With this in mind, it is suggested that the Formosan data protection regulators as well as law practitioners should adopt a broad conception of privacy. It seems that Formosan constitutional interpretation welcomes such an idea by reading J. Y. Interpretation Nos. 535 and 603. However, the recent constitutional interpretation seems to be hesitant on this. In J. Y. Interpretation No. 689, although the Honourable Judges consider that the rights at issue include spatial privacy (bodily integrity and the right to be let alone) and informational privacy respectively, they do not apply the idea of privacy to deal with the debate between 'private actions' and the freedom of media.[63] Nevertheless, this can still be seen as a starting point – not satisfying but encouraging – of the acceptance of a broad concept of privacy.

[61] Paul M. Schwartz and Daniel J. Solove, 'The PII Problem: Privacy and A New Concept of Personally Identifiable Information' (2011) 86 NYU Law Review1817, 1873-1877. See also: Ulrich Dammann, *Kommentar zum Bundesdatenschutzgesetz* (Spiros Simitis ed, 6th edn, Auflage 2006) §3, cited from Schwartz and Solove (n 61) 1874.
[62] Section 3.6.
[63] Chien-Liang Lee, 'The Conflict and Balance between the Freedom of Media and the Protection of Private Life: Brief Comments on J. Y. Interpretation No. 689' (2011) 184 The Taiwan Law Review 38.

2. Consent

It is observed that

> Where a data protection regime is underwritten by an ethic of rights and where (as I take it) the ethic is based on a choice (or will) theory of rights, there is no escaping the fact that consent must be central to that regime.[64]

In this light, the principle of the priority of consent could be applied in the Taiwanese data protection regime. Hence, where possible and practicable, consent should be obtained from each agent (data subject) prior to the collection, processing and use of personal data. However, it is noted that the confusion around the integrity of consent under the PDPL as well as in other places of the legal regime must be put right.[65] In this case, the two Fallacies of consent should be prevented. There are indeed a series of best practices that the European data protection model requires in obtaining consent that are practicable, for example:[66]

1. Consent procedures should be designed to obtain *valid* and *sincere* consent: data subjects must be given sufficient and accurate information in order to make a decision that reflects their voluntarily wishes; they must be given sincere opportunity to ask questions and have these answered; and they must not be subject to coercive measures. This has been noted in the 2012 data protection rules reform: whenever consent is required for data processing,

[64] Roger Brownsword, 'Consent in Data Protection Law: Privacy, Fair Processing and Confidentiality' in Serge Gutwirth and others (eds), *Reinventing Data Protection?* (Springer 2009) 87.
[65] Section 6.4.1.
[66] Scottish Health Informatics Programme (SHIP) (n 59) 5.

consent has to be given explicitly rather than be assumed.[67]

2. Where there are prospects of future use of data that are unknown/ uncertain at the time of consent, then data subjects should be informed of the broad/ possible purposes for which said data might be used.

The above measures reflect a will-based reasoning to keep faith with the agent's free will. The first point is particularly crucial with respect to biometric applications, whilst the second should be carefully considered to avoid the function creep of RFID applications. It must be noted that with respect to the second point regarding informed consent, I am not suggesting that data subjects should be informed about 'everything' that could happen in future processing. This is simply because it is impossible to do so, as the nature of the progress and impacts of science and technology can never be fully anticipated.

Indeed, since sensitive personal data should be placed in a higher hierarchy, the suggestions outlined above should be applied more strictly on a proportional basis with regard to biometric applications. We have seen that the unique cultural dynamics in Taiwan that cause confusion are based on the problematic understanding of public interest. It seems to me that Formosan regulators should make this clear and borrow practicable experiences from the European model, e.g., recent reform proposals, in particular on how to avoid confusion on the integrity of consent.

[67] It is stated in Recital 25 of the proposed General Data Protection Regulation that: 'Consent should be given explicitly by any appropriate method enabling a freely given specific and informed indication of the data subject's wishes, either by a statement or by a clear affirmative action by the data subject, ensuring that individuals are aware that they give their consent to the processing of personal data, including by ticking a box when visiting an Internet website or by any other statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of their personal data. Silence or inactivity should therefore not constitute consent. Consent should cover all processing activities carried out for the same purpose or purposes. If the data subject's consent is to be given following an electronic request, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided.'

Where obtaining consent is not reasonably possible/ practicable, on the other hand, anonymisation of data as a type of PETs can be taken into account.[68] However, the appropriateness of this course of action is limited, since the possibility of re-identification of personal data is increased by rapid developments of biometric and RFID technologies. Moreover, it has been said that advances in information science have made anonymisation 'a broken promise' which fails to protect personal data.[69]

3. Trust

I have argued that it is better if obtained through sincere trust to move agents to give/acquire valid consent.[70] Hence, regulators should try to craft mechanisms for building trust in their agents.[71] Rules reflecting the necessity for better trust are also encouraged. To keep faith with the agent's free will, the need for responsibility and accountability of data processing in relation to the applications of new technologies should always be taken into account. In this regard, the EU data protection reform offers an increased responsibility and accountability for data processing, e.g., the duty to notify the national data protection supervisory authority with respect to serious data breaches as soon as possible.[72]

In the 2012 EU General Data Protection Regulation proposal, it is pointed out that there are worries on behalf of the data subjects in relation to the loss of control of their personal data, which 'eats away at their **trust in online and other services** and

[68] Laurie and Sethi (n 59) 58.
[69] Paul Ohm, 'Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization' (2010) 57 UCLA Law Review 1701.
[70] Section 7.3.2.
[71] Ohm (n 69) 1767.
[72] Articles 31 and 32.

holds back the growth of the **digital economy** in general.'[73] (original emphasis) Accordingly, a series of new rules are suggested in the proposal in order to gain more power of control for data subjects: data subjects will have easier access to their own personal data; the right of data portability, i.e., easier to transfer of personal data from one data controller to another; and the 'right to be forgotten,' i.e., the possibility to delete personal data if there are no legitimate grounds for retaining it. These new rules with respect to data subjects' power of control over their personal data not only favour the trust element of data processing, but also reflect the rule-preclusionary conception of property. This is therefore encouraged.

Further supplementary measures to enhance the co-operative model are also suggested to deal with uncertain and identified risks of the technologies at hand. In the EU data protection reforming proposal, this is coupled with the principles of 'privacy by design' and 'privacy by default.'[74]

PIA is a practicable instrument for identifying/ monitoring potential privacy risks prior to the implementation of any particular model.[75] PETs as well as good data protection practices, e.g., transparent controls and security processes which are the data controller's responsibility,[76] are also recommended in the general guidelines. This is in line with Article 17(1) of the Data Protection Directive which requires that data controller must efficiently implement measures, including technological provisions (e.g., PETs) and organisational ones (e.g., PIA), which 'ensure a level of security

[73] European Commission, 'Why Do We Need an EU Data Protection Reform?' (2012) <http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/1_en.pdf> accessed 30 Janurary 2012.
[74] Article 30(3) of the General Data Protection Regulation proposal.
[75] Laurie and Sethi (n 59) 59.
[76] It is suggested that although 'it is possible that these policies may not be developed solely by data controllers, but in conjunction with others, e.g. lawyers, but ultimate responsibility for implementation of such policies will lie with the data controller.' Scottish Health Informatics Programme (SHIP) (n 59) 3.

appropriate to the risks represented by the processing and the nature of the data to be protected.' Indeed, according to Borking, PETs have to be applied 'for implementing the legal specifications in the EU privacy directives 95/46/EC and 2002/58/EC, like data minimization, consent requirements, access rights of data subject, privacy safe construction of terminals in information systems.'[77] Moreover, Koorn and others observe that one of the advantages offered by the utilisation of PETs is that it 'signals trustworthiness, and creates public confidence in the processing of their personal data in government information systems.'[78]

However, in practical applications, there are factors affecting the adoption of PETs. For example, in their contribution Klüver and others contend that PETs, so far, have not been applied as broad as possible because of lacks of availability of PETs and user friendliness.[79] Nevertheless, Borking suggests that '[g]ood education concerning the technical possibilities of PETs and concrete requirements in the legislation (such as a privacy impact or threat analysis assessment) is necessary for promoting the PETs applications.'[80] In his article on the basis of the empirical approach, he concludes that there are two crucial issues affecting the adoption of PETs: (1) the positive factor, i.e. legal and regulatory pressure regarding privacy protection, and (2) the negative factor, i.e. costs for investment in PETs.[81] To solve the negative issue, he proposes to consider investments in PETs as 'regular investments,

[77] John J. Borking, 'Why Adopting Privacy Enhancing Technologies (PETs) Takes so Much Time' in Serge Gutwirth and others (eds), *Computers, Privacy and Data Protection: an Element of Choice* (Springer 2011) 310.
[78] Ronald Koorn and others, *Privacy Enhancing Technologies –White Paper for Decision-Makers* (2004) 1, 6.
[79] Lars Klüver, Walter Peissl and Tore Tennøe, *ICT and Privacy in Europe: Experiences from Technology Assessment of ICT and Privacy in Seven Different European Countries* (EPTA 2006) 41. Borking (n 77) 311-312.
[80] Borking (n 77) 338.
[81] Ibid 314-327.

characterized by cash flow patterns.'[82]

Moreover, in order to promote public confidence, high standards of research and application practice should be met during all aspects of the research process.[83] However, the two mechanisms remain underdeveloped in the Formosan data protection regime. The introduction and further training for both the data controllers and data subjects are thus needed. These mechanisms, for this purpose, should be better communicated both to the public and to oversight bodies/ individuals with responsibility through an independent authority, which is yet to be established in Taiwan.[84]

Lastly, public engagement is an integral part of good governance in relation to the trust between data controllers and data subjects. Hence, active engagement exercises should be developed and implemented. Moreover, such an engagement includes stakeholder engagement for *private* applications for technologies at issue. Again, public interests and expectations 'should be monitored over time by an appropriate body or individuals with appropriate expertise for the task.'[85]

4. Balancing Interests and Rights

(i) State responsibilities and individual rights

Under the PGC, agents possess any given generic rights and are under the duty to respect the generic needs of an agent. The duty to respect generic rights of all agents,

[82] Ibid 339.
[83] Laurie and Sethi (n 59) 59. Article 29 Data Protection Working Party, *Opinion 3/2012 on Developments in Biometric Technologies* 34.
[84] For further suggestions, see section 8.3.2.
[85] Scottish Health Informatics Programme (SHIP) (n 59) 16.

in particularly the positive rights of agents, must consider the empirical conditions of their possible implementation.[86] In the light of the universality of the generic rights, the implementation of generic rights rests on the shoulders of various governmental institutions in order to secure/ promote the rights.[87] However, it should be emphasised that 'these institutions function as *representatives* of individuals, who are in this way jointly responsible for providing the needed assistance.'[88] (emphasis added) The agents here are, in principle, those *ultimately* responsible for the generic rights.[89]

Accordingly, the prevention of abusing State powers to implement the protection of generic rights must be taken into account and reviewed at all times. We have mentioned in section 8.2.2 that the Taiwanese hybrid legal regime is profoundly influenced by the traditional Chinese value of sacrificing oneself for the sake of the whole. This leads to misinterpretations and incorrect implementations that the responsibility of states to protect individuals' fundamental rights and freedoms

(1) is the basis of fundamental rights and freedoms of agents; and

(2) could override fundamental rights and freedoms of agents.

The first mistake is self-explanatory, since governmental institutions operate as *representatives* of individuals. As regards the second fallacy, we must not forget that such duties logically originated from the duties of agents to implement the generic rights. Only a generic right/ fundamental right and freedom can override another generic right/ fundamental right and freedom according to the criterion of degrees of needfulness for action when the two rights are in conflict. It is crucial to appreciate that we should not make the mistake to consider the generic rights of an agent, which

[86] Gewirth, *The Community of Rights* 55.
[87] Ibid 55.
[88] Ibid 55.
[89] Ibid 56.

might be able to limit/ override a generic right, as the duty of States.

(ii) Balancing the interests between academic research/ enjoyment of advances of science and technology and privacy: the precautionary model

The second issue to be taken into account is how to avoid the worship of privacy and the worship of academic research/ enjoyment of advances of science and technology in the Formosan legal regime. It is observed that there is a tendency for Taiwanese regulators to make judgements on scientific developments by assuming that no unwanted risk would occur merely from applying the 'mature technology.' In other words, it seems that a 'small risk' of the violation of privacy is offset by the benefits in everyday life and economic profits. In this case, biometric and RFID applications thus are interpreted as being subject to strict data protection regulations only when the end applications are clearly not substantially equivalent to their expected performances/ interests.

It is therefore unsurprising that with respect to privacy debates concerning such research and its applications, Formosan scientific researchers (as well as global scientists) argue that the technical solution of anonymisation is able to respond to the privacy concerns. This is reflected by Article 18 of the Human Biobank Management Act.[90] This seems quite similar to the American (including the U.S., Canada and Argentina) attitude in relation to the GM corps,[91] which seems to be more or less in favour of scientific applications. The purpose of this thesis is not to judge the approach chosen by the Taiwanese regulator. However, as I have said, the possibility

[90] Article 18.I states that 'Any storage, use, or disclosure of the concerned operator's entire biological specimens and related data and information shall be encoded, encrypted, delinked, or transformed so that the participant's identity is unable to be determined.'

[91] See: Deryck Beyleveld and Roger Brownsword, 'Complex Technology, Complex Calculations: Uses and Abuses of Precautionary Reasoning in Law' in Paul Sollie and Marcus Düwell (eds), *Evaluating New Technologies* (Springer 2009) 187-189.

of re-identification on such data is expending due to the development of technology. How to deal with the problem brought by the massive amounts of personal data? What suggestions (a coherent set of the PGC-compliant regulation) should the thesis propose on the basis of the theoretical framework chosen?

Let us revisit the precautionary reasoning on the PGC ground as the starting point.[92] I argue that the principle should be considered with respect to the growing scope of personal data (or, PII). This is because it is useful in dealing with the uncertain privacy risks brought about by the capacity of re-identification. Indeed, the principle is formulated by the Nuffield Council on Bioethics in relation to the concerns over genetically modified crops that the regulators may 'impose restrictions on otherwise legitimate commercial activities, if there is a risk, even if not yet a scientifically demonstrated risk…'[93]

However, there are a handful of general objections to the principle in relation to the complexity of technology, for example, (1) the degree of scientific uncertainty; (2) the types of risk; (3) the degree or character of the perceived hazard; and (4) the measure of precaution to be taken.[94] Specifically, the central idea of the principle rests on the assumption that actions are to be avoided 'simply because they *might possibly* threaten wholly unacceptable outcomes.'[95] The uncertainty of the failure and risk stemmed from technologies, arguably, can be minimised by the development of science and technology. The expansion of the protection of personal data (the European data protection approach) therefore seems to be overreacting to some

[92] Cf. section 3.2.3.
[93] Nuffield Council on Bioethics, *Genetically Modified Crops: The Ethical and Social Issues* (Nuffield Council on Bioethics, 1999) 162.
[94] Beyleveld and Brownsword, 'Complex Technology, Complex Calculations: Uses and Abuses of Precautionary Reasoning in Law' 178-180.
[95] See Beyleveld and Brownsword's introduction to 'Pascal's Wager.' Ibid 181.

commentators.

To respond to these objections and justify the ***precautionary model*** for the Formosan data protection regime, let us recall what was presented in the theoretical part of the thesis.[96] The PGC is a moral principle requiring a set of categorically obligatory imperatives for action, which is binding on all agents. We have said that the fundamental rights and freedoms protected by data protection laws are generic rights. A broad conception of privacy (i.e. the expansionist approach described by Schwartz and Solove)[97] therefore is essential to avoid the violation of the right to privacy as well as the generic rights protected by data protection law. This is because, according to the precautionary reasoning, to violate a generic right by mistaking a generic right for non-generic right causes more harm than mistaking a non-generic right as a generic harm under the PGC, as the PGC requires the prevention of generic harm. The European data protection model to regard identifiable data (including that which may possibly be re-identified) as personal data is thus reasonable.

However, it is noted that the protected rights and freedoms are not absolute. Thus, according to precautionary reasoning and the criterion of degrees of needfulness for action, although identifiable/ re- identifiable data should be included within the scope of personal data (in a broad-concept sense) to avoid the risk of violating privacy, it needs to be proportionately treated on the basis of the possibility of being identified. Nevertheless, it is noted that, as the WP29 puts, '[i]n cases where biometric data, like a template, are stored in a way that no reasonable means can be used by the controller or by any other person to identify the data subject, those data should not be qualified

[96] Chapter 3.
[97] Schwartz and Solove (n 61) 1817.

as personal data.'[98]

To sum up:

1. If data refers to an identified agent, the risk level is the highest.
2. If data refers to an identifiable agent, the risk level is lower than the identified one. Since there remains a possibility of risk, minimising the risk of violating generic rights (e.g. privacy) is still needed. It is noted that according to the criterion of degree of needfulness for action, since the risk of identifiable data is lower than that of identified data, to protect the competing generic need (e.g. the right to enjoy the advances of science and technology), such data should be proportionately less limited than identified data.

Such a distinction between identified and identifiable data is particularly relevant to the Formosan data protection regime, which seems to be hesitating to totally accept the European data protection model.

8.3.2 The Regulatory Attempts (II): The Institutional Framework

It was suggested in Chapter 7 that an independent data protection institutional framework could better apply the co-operative model in practice. However, it has been pointed out that although the Formosan data protection legal regime borrows a certain number of experiences from the European model,[99] there is no single authority

[98] *Article 29 Data Protection Working Party*, (n 83) 5.
[99] In the 2012 EU General Data Protection Regulation proposal, it is stated that an independent supervisory authorities in Member States are essential to protect personal data. Recital 92 of the document: 'The establishment of supervisory authorities in Member States, exercising their functions with complete independence, is an essential component of the protection of individuals with regard to the processing of their personal data. Member States may establish more than one supervisory authority, to reflect their constitutional, organisational and administrative structure.'

with complete independence in charge.[100]

The imaginable and foreseeable disadvantages of the hydra-headed bureaucracy model are not difficult to identify. For example, it has been observed that the model applied in Taiwan may generate inconsistent data protection implementations.[101] However, by not establishing a new public authority, public spending is reduced; therefore, the model might be justified in the context of austerity measures. Nonetheless, this goal can hardly be achieved by taking the current model applied in Taiwan, as the cost to taxpayers still needs to be invested in vertical and horizontal communications within the governmental authorities to solve problems of the hydra-headed bureaucracy model.

Furthermore, the central problem of the hydra-headed bureaucracy model lies on the issue of whether the responsible authorities are *capable* and *credible* in being in charge of data protection matters. Let us take J. Y. Interpretation No. 689 as an example.

It is stipulated in Article 89 (2) of the Social Order Maintenance Law that a fine can be imposed on individuals who trace others without justified reasons and fail to desist from trailing/ stalking after valid warning. The applicant is a show-biz reporter who trailed and took pictures of celebrities. After being advised to stop such behaviour, the applicant continued engaging in these activities. The investigation and decision on whether or not to penalise the trailing act is held by the policing sector. In relation to the issue of striking, a balance between the freedom of media and the right to privacy and personal data protection, the majority opinion rules that the freedom of media is not an absolute right and thus can be restricted. It is justified by the

[100] Section 5.3.3.2.
[101] Section 5.3.3.2.

requirements including a number of ‘public interests’ and the intolerance on the basis of ‘social norms.’

Although the Honourable Judges hold that the rule is constitutional,[102] the Court advises relevant authorities to re-consider whether it is appropriate to leave the policing sector to decide such matters. This is because, it reasons, such penalising power is indeed rather complex for the policing sector to exercise. The Honourable Judges further suggest that the authorities should take into account whether it is appropriate to have courts render the direct decision in order to ensure the efficacy of governmental authorities and balance between the freedom of media and personal data protection, with particular reference to the right to privacy.

By applying the hydra-headed bureaucracy model, it might be said that it is easier for the policing sector to manage and respond to urgent violations of generic rights. However, the expertise and capabilities of the police authorities, as suggested by the Constitutional Court, must also be taken into account – after all, it deals with rather complex questions concerning fundamental rights and freedoms.[103] Furthermore, the European data protection and privacy model is indeed rather ‘burdensome’ to not only data controllers but also to governmental agencies. A specialised institution that can take full responsibility for these issues would thus be appropriate.

In addition to establishing an independent Formosan data protection supervisory authority with adequate functions, ‘adequate financial and human resources, premises

[102] It is noted that it remains dubious whether the Interpretation achieves the purpose of striking a balance between the freedom of media and the right to privacy. See, e.g., Lee (n 63) 29-49.
[103] It seems that the alternative choice may be the Ministry of Justice to decide such matters. However, we have also said that the Ministry of Justice cannot play such a role properly since the independency of the department is remaining doubtful. See: section 8.2.4.

and infrastructure,'[104] I suggest that

1. An advisory board for the creation of an independent institution should be formed. The composition of the board of experts should include members from diverse backgrounds who possess the necessary expertise in not only data protection law field, but other fields, e.g., technological, social-economical expertise, in order to make appropriate and justifiable decisions. This is particularly crucial when drawing up technical standards in relation to privacy by design and by default PETs. Moreover, as the WP29 suggests, appropriate consultations with respect to external technical experts, e.g., international standardisation organisations, are recommended.[105]
2. This institution should offer appropriate training modules to data controllers (including governmental agencies) as well as data subjects. Appropriate reviews of the practices should be carried out.
3. An optimal model would include investigative powers, effective powers of intervention, the power to engage in legal proceedings and the power to appropriate.[106]

Such guidelines should be able to assist the success of the co-operative model.

[104] European Commission, '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)' (2012) <http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf> accessed 30 Janurary 2012, Recital 94.
[105] Article 29 Data Protection Working Party, *Opinion 01/2012 on the Data Protection Reform Proposals* 11.
[106] Cf: Recital 100 of the proposed EU General Data Protection Regulation: 'In order to ensure consistent monitoring and enforcement of this Regulation throughout the Union, the supervisory authorities should have in each Member State the same duties and effective powers, including powers of investigation, legally binding intervention, decisions and sanctions, particularly in cases of complaints from individuals, and to engage in legal proceedings. Investigative powers of supervisory authorities as regards access to premises should be exercised in conformity with Union law and national law. This concerns in particular the requirement to obtain a prior judicial authorisation.'

8.4 Summary

I have compared the data protection regulations in both legal regimes with a particular focus on the technologies at issue. It has been shown that although it roughly applies the European data protection model, the current Formosan data protection framework has its own unique problems with respect to the applications of biometric and RFID technologies. Since we have seen that the European model roughly matches the PGC requirements, it is suggested that the Formosan data protection framework needs no major revision in order to meet the new challenges brought about by the advanced technologies at issue – in other words, there is a need to strong argument to re-affirm the European model in the Formosan data protection regime. However, minor corrections to improve reliability of data processing are called for, in particular a consistent approach to maintaining valid consent, precautionary and preventive measures against risks of developing such technologies, and an independent institutional framework.

Chapter 9

Conclusion

9.1 Answering the Research Questions

The central aim of this thesis is to examine how to strike a balance between the benefits and the risks of biometric and RFID technologies within a data protection regime. Throughout this thesis, I have sought to provide an answer to this question. By way of conclusion, it is time to assess whether this thesis has met its proposed aims and review its findings in response to the research questions listed at the start.

Chapter 2 provided an essential overview of biometric and RFID systems and their omnipresence in people's daily lives. This included key terms, the promised benefits and the potential risks of these technologies. The data protection concerns discussed with respect to the technologies at hand presented four notable themes: **the concept of privacy, consent, trust, and interests-balancing issues between public goods and individual interests**. Having set out the background, the thesis then turned to its main theme.

1. **Identifying and justifying an adequate theoretical framework to deal with the question**

To deal with data protection concerns, researching how to strike a balance between the concerned rights and their competing rights generally raises numerous conceptual questions, which are intensified in relation to emerging technologies. In particular,

this particularly raises the question of the choice, justification, and applicability of the theoretical approach adopted. **Chapters 3 and 4** dealt with this question.

Indeed, there is a rich variety of theoretical evaluations to contend with. The theoretical framework chosen in this thesis is the Principle of Generic Consistency. The PGC has been briefly illustrated, focusing on concepts of the agents, generic rights and the relationships between the two concepts in **Chapter 3**.

A convincing justification of a single theory can at least prevent blind spots where the chosen ethical theory is not well developed and the risk of inconsistency. Two arguments have been presented in relation to the justification of the theoretical framework. By applying the dialectically necessary argument to the concept of agency in three stages, the PGC has been justified as the basic principle of human rights in any community, requiring agents to act in accordance with the generic rights of all agents. However, some are sceptical towards this theory. Most of them focus their critiques on stages II and III, in particular the ASA and the LPU.[1] Nevertheless, the dialectically necessary argument has not been convincingly countered, as most of the suggested flaws are misunderstandings.

Even if the flaw has been identified and explained, I have presented the dialectically contingent argument to deal with this. On the basis of this method, any legal regime which recognises human rights and is based on the assumption of impartiality must grant the PGC a similar status, or else contradict acceptance of such recognition. Overall, very few objections are insurmountable. However, it must be noted that rather than defending or providing a full analysis of this moral theory, the primary mission of this thesis is only to apply the PGC to produce clear guidelines

[1] Section 3.1.

and principles to strike a balance between the benefits and the risks of biometric and RFID technologies within a data protection regime.

The generic needs of agency are hierarchical. Fundamental rights and freedoms, such as the right to benefit from advances in science and technology and the right to privacy, are prone to coming into conflict. In Chapter 3, direct application of the PGC as the general methodology to reconcile competing rights and interests was presented.

The following chapter moved on to elaborate a specific application of the PGC to select issues. **Chapter 4** first defined the field of privacy concepts and then described how it has been analysed to allow the identification, evaluation, and comparison of competing rights and interests in a specific conflict.

It has been argued that, with respect to the concept of privacy, reductionist theories are not capable of dealing with the issues of current and future development of the right to privacy. I have further argued that it is unwise to tag or limit the concepts of privacy and becloud oneself to the extension of the concepts of privacy at the stage of identifying and valuing rights covered by the notion of privacy. I have indicated a plethora of different rights that fall under the heading of the right to privacy by using the categorisation deriving from Allen. However, the impossibility of an exhaustive definition of privacy, which is intensified by the emergence of new technologies, raises questions of inconsistency and instability. Nevertheless, the PGC provides a rationale to assist in identifying generic rights covered by privacy.

Moreover, the problem of inconsistency and instability with respect to the approach of balancing test applied by courts can be solved by applying the criterion of degrees of needfulness for action. After indicating that the ECHR is in line with the

PGC, I have shown how the criterion operates in practice by taking the *Marper* case before the ECHR as an example. On the basis of this criterion, as generic rights are ranked hierarchically, I have argued that the criterion here offers a role as the law of gravity (gravitation), which gives weight to objects with mass according to degrees of needfulness for action. Some points have to be noted in this respect. First, as a collective right within a community/ society presents a right which is designed to improve the benefits of all agents in such a community/ society, the criterion ought to be able to deal with the collective right or the public good.[2] Secondly, the criterion here is concerned with preventing violations of necessary means of agency (including *harms* consisting in removing or threatening the basic, non-subtractive, or additive rights available to all agents), rather than increasing the benefits. Thirdly, it should be noted that, unlike the utilitarian argument, if a generic right is more needed for action than another generic right, the former will not be overridden by the latter – even if the latter one is relevant to a large number of agents.

2. Probing and evaluating current regulations of biometric and RFID technologies in Europe and Taiwan

Chapters 5 and 6 were devoted to fulfil the mission of probing and evaluating current regulations of biometric and RFID technologies in Europe and Taiwan. Any research in connection to the context of global data protection law regime must carefully explore the European model. With this in mind, The Data Protection Directive is definitely a significant milestone worth analysing. This part examined themes in relation to consent and the balancing of different interests such as public goods and individual interests, the institutional framework of reference and the relationship between the Directive, the ECHR and the Data Protection Convention.

[2] Alan Gewirth, *The Community of Rights* (The University of Chicago Press 1996) 48.

Moreover, the application and the domestic influence of the European data protection model have also been discussed.

On the other hand, the position of the right to privacy and personal data protection with respect to the regulatory mechanisms for modern technologies in Taiwan has also been outlined. Although a legal foundation regarding the right to privacy in Taiwan is relatively weak due to the profound cultural influences of both the Chinese immigrants and the Nationalists Party (KMT), there has been a demand of judicial effort with regards to the emerging rights and interests. The PDPL is a major player in this regard. Moreover, the concept of privacy in the Formosan legal regime was examined. As regards specific data protection law regarding biometric and RFID applications, it has been observed, unsurprisingly, that there are relatively few regulations in both regimes.

On the basis of the legal issues highlighted so far, I have identified a number of questions to be evaluated. Before the evaluation, I argued that both the European and Formosan legal regimes are in line with the PGC and can be considered as a clear application and the two communities are competent decision-making bodies applying the PGC. In **Chapter 6**, I replied each question in turn. First, I argued that there is indeed a generic right to benefit from science and technology. This is because, in the light of the PGC, vast fields of technologies bring about improvements which increase the overall general chances of success. Also, this right has been recognised in relevant international human rights instruments. However, as such rights to generic conditions of agency impose obligations to the other agents, they potentially conflict with the other agents' generic rights. Moreover, due to the nature of the rights at issue, it can also cause harm to other rights to generic condition of agency. This leads to the second issue identified: the data protection concerns, in particular the right to privacy,

brought by modern technologies.

As previously mentioned, I adopted Allen's categorisation as a general application to examine the concepts of privacy. With respect to spatial privacy, firstly, I argued that, given that an agent acts through its own body, to violate the integrity of her/his body can generically affect her/his capacity to act at all or act successfully. A generic right to bodily integrity should thus be granted. Moreover, it is not a sincere grant to afford an agent's right to have bodily integrity without granting them to control their body. However, this does not follow the recognition of control over *subsequent* uses of their body. Nevertheless, the *functional* aspect of the claim for such a question should be taken into account for the analysis of the right to bodily integrity in relation to the concept of the right to privacy, particularly when the research/ application focuses on the *subsequent* uses of the body parts. In this respect, I adopt Beyleveld and Brownsword's justification for property rights, i.e., the 'rule-preclusionary' conception of property,[3] and suggest that biometric samples would imply exclusive use, subject to the waiver (with valid consent) or the overriding rights of others, whether individually or collectively, without bargaining the specific right in every particular use.

In the light of decisional privacy, I have argued that to deny an agent's decisional privacy by acting against its free and voluntary choice, either those decisions concerning only its/her/his own business, or establishing or changing relationships with others, amounts to a violation of the PGC. Moreover, it should be noted that it is by virtue of vulnerable agency that the generic rights are to be granted and impose duties on other agents to respect the generic rights of the right-holder, rather than a

[3] Deryck Beyleveld and Roger Brownsword, *Human Dignity in Bioethics and Biolaw* (OUP 2001) 171-194.

protection from external interferences. Therefore, the collection and processing of biometric data and the employment of RFID technology should not be seen as freeing an agent from social or legal constraints. Rather, we should regard an agent as an end who independently and voluntarily acts for any kind of purposes.

In respect to informational privacy, I have discussed the 'nothing to hide' argument. I have contended that regardless of the purpose, for example, of whether the agent wants to hide something sensitive, embarrassing, illegal, or even to hide nothing, there is a generic right to informational privacy – if the purpose is valuable/ good to it. Moreover, it is correct that the concealment of negative matters cannot cover all aspects of the notion of privacy. However, this is by no means conclusive as the negative/wrong matters, which may place an agent at risk, can still be the purpose of action without violating a right. Furthermore, the 'nothing to hide' argument fails to take certain informational rights into account, such as the right to know and control how personal information will be used, and the right to correct any inaccurate entries contained in stored information, the right to decide whether or not to disclose information, the right to know and control how personal information will be used, and the right to correct any inaccurate entries contained in stored information.

To adequately focus on the specific forms of privacy that are relevant to the thesis, it is crucial to note that it is a right profoundly affected by modern technologies. I have addressed that in the cases in which: (1) an agent does not *know* that their information has been processed; and (2) new technologies are used as a medium to disclose an agent's information against their will, the agent's generic rights are violated. With regards to the substantial changes brought about by cutting-edge information and communication technologies that provide motivations for agents to disclose/ share information with others, this is not forbidden by the PGC. This is

because there are no direct duties to oneself under the PGC – the benefits of the generic rights can always be *freely* waived – provided that this waiving does not threaten the generic rights of others.[4]

How to deal with competing rights that conflict with one another is the central issue to be examined. Both procedural and substantive justifications are allowed under the PGC. With respect to consent as the procedural justification, we should neither overestimate nor underestimate the function of consent. What should be emphasised is the use of consent in the correct context. Accordingly, we should prevent from committing the Fallacy of Necessity as well as the Fallacy of Sufficiency. Two further issues need to be clarified. First, consent should be regarded as a safeguard operating as a defence rather than as a cause of action.[5] In this respect, the priority of consent should always be born in mind. Secondly, the function of consent as a procedural justification must not be confused with substantive justifications. Consent authorises the action for the consent receiver does something to the consent giver, it thus follows that the consent receiver does no wrong to the consent giver.

On the basis of the groundwork on consent, I argued that the confusions surrounding the integrity of consent under the PDPL should be clarified. As consent can reflect individual autonomy to some extent, it should be a root justification with respect to sensitive personal data.

With regards to the substantive justification to the right to academic research and its benefits in the data protection law regime, it has been noted that the equation shall rest firmly on the generic conditions of agency. Here, on the basis of the direct application of the PGC, we assess the reconciliation of competing rights by applying

[4] Ibid 194.
[5] Deryck Beyleveld and Roger Brownsword, *Consent in the Law* (Hart Publishing 2007) 242.

the criterion of degrees of needfulness for action. However, it should be noted that the critical point is whether such a 'public interest' is proportionately regulated by effective safeguards, such as strict rules or anonymisation of data to approval through the institutional framework when these competing rights and interests come into conflict. More importantly, again, the outcome of any balancing test shall not favour the opinion that a substantial serious harm to a particular agent is outweighed by the sum of individually negligible goods for the other agents within the collective group.

3. Providing clear guidelines and principles for legal regulations to deal with the two technologies at issue

It has been contended that balancing tests under a conflict model tend to exclude the possibility that both interests at issue can be fostered and protected in an optimal way, since a balancing test is generally viewed as weighing one interest against the other. In this light, there is a risk that the value of consent is diminished to the extent that individual rights and human dignity are undervalued or even ignored.

However, it is problematic to suggest that the balancing of competing rights is a zero-sum trade-off. Instead, in line with a broad concept of privacy, it has been argued in **Chapter 7** that there is the possibility of two sets of values being capable of supporting each other.[6] This is because, on the one hand, the fulfilment of data protection requirements, and in particular the protection of the right to privacy, can support applications of modern technologies; on the other hand, the applications of

[6] Deryck Beyleveld, 'Conceptualising Privacy in Relation to Research Values' in Sheila AM McLean (ed), *First Do No Harm: Law, Ethics and Healthcare* (Ashgate Publishing 2006) 156-158, and Deryck Beyleveld, 'Data Protection and Genetics: Medical Research and the Public Good' 18 King's Law Journal 275-289.

modern technologies can improve security and convenience of private life of individuals (which are also privacy values) as well as the public interest.

With respect to the justification of the co-operative model, as the acceptance of a broad conception of privacy is a prerequisite of the co-operative model, the justification of the acceptance of a broad concept of privacy will justify this model.[7] Apart from the legal justification in relation to the two data protection regimes addressed in Chapters 4 and 5, there are also ethical and pragmatic reasons. The first step is to relate the relationship between *privacy and benefits from advances in science and technology* to the relationship between *data subjects and data controllers*. Under the PGC reasoning, data subjects must be treated as ends and possess both negative and positive rights. Accordingly, both parties share the common interests of the two rights and interests: the two parties should, therefore, work as partners since there is mutual respect for rights of both parties.

This is also in line with the pragmatic justification. To assess the pragmatic reason in a detail, we can take game-theory ideas into account to explain behaviours of partners (data subjects and data controllers) in contexts where the outcome of actions depends on how agents chose to act. By doing so, I characterised the situation as a prisoner's dilemma. In this case, it can be argued that without any cooperation, the agents involved in data collecting, processing and using are prone to coming into conflict. As regards the enhancement of the co-operative model, I argued that all of the suggested strategies are closely related to the trust between rights holders. In other words, through the way of satisfying each other by treating others as oneself, it is possible to enhance incentives to improve cooperation. However, it should be noted that, on the basis of game-theoretic thinking, the full avoidance of generic harm is the

[7] Beyleveld, 'Conceptualising Privacy in Relation to Research Values' 158.

highest-ranked outcome – although this is not always possible. In other words, there is a possibility of conflict within the co-operative model. Nevertheless, it is recalled that provided that valid consent is obtained, there is no need to deal with subsequent substantive justifications. Hence, with respect to the co-operative model, valid consent is a crucial key which serves as a device to show respect to fundamental rights and freedoms.

With this in mind, I have demonstrated two key privacy and data protection enhancing mechanisms, which espouse the practicability of the co-operative model, namely PIA and PETs. Applying these frameworks, I suggested that a well-designed structure with an early engagement of the two mechanisms is capable of improving trust between participants of the collection and processing of personal data. Moreover, the risk of violating generic rights can be minimised in so far as it is possible to do so. This is because risks could be more easily assessed in the initial stages since any control or change is difficult when the technology has become entrenched further. It is noted that, in this regard, risk assessment includes two types of risks, namely the identified and the uncertain ones. The former ones can be dealt with preventive measures, while precautionary assessments are employed to identify uncertain risks.

However, PETs do not necessarily protect privacy effectively. First, under a broad concept of privacy, the right to know one's personal implications for oneself is rendered impossible by the design of PETs. Moreover, anonymised data is less valuable for such technologies. Furthermore, it is unrealistic to expect that technical methods can actually keep personal data confidential and in line with *all* data protection principles. This is particularly true when processing data via internet or intranet because there is no trust on the internet. To deal with this, I have argued that the improvement of opportunities for consent and enhancement of its meaningfulness

by taking account relevant social practices are capable of dealing with the problem. Hence, technologies which can achieve the above purpose are also PETs.

In the light of regulating biometric technologies, I have said that it is at least arguable that there is a need to draw efficient regulations. This is because although it might be argued that commentators may hold differing opinions towards emerging technologies, an overconfident attitude without appropriate legal architecture to ensure a responsible approach to research and innovation is by no means an accurate way to consider the consequences if they fail.

Moreover, I argued that a more 'burdensome' data protection regulatory model which is in line with the European data protection model, rather than the minimal-regulating model, should be encouraged.

A number of complex desiderata must be taken into account in terms of regulatory design. In the light of the flexibility of the regulatory instruments, it has been argued that a lighter regulatory model can be applied to rights and interests that can be given equally.[8] Also, this model can be applied to those will not qualify as earth-shaking matters of justice or morality on Gewirthian grounds (at least for those does not prohibited by the PGC). As regards the rights and interests cannot be given equally and those possess a clear violation against generic conditions of agency to an open future, on the other hand, a more rigid regulation is *proportionally* demanded. In this regard, attention should be firstly paid to consent without resorting to Fallacy of Necessity and Fallacy of Sufficiency arguments. Hence, the efficiency and validity of consent is crucial for the regulatory design. Moreover, in pursuit of a smart regulatory

[8] Deryck Beyleveld and Shaun D. Pattinson, 'Individual Rights, Social Justice, and the Allocation Of Advances in Biotechnology' in Michael Boylan (ed), *Public Health Policy and Ethics* (Kluwer 2004) 66.

design, I suggested that regulators should consider elements such as the respect for users and controllers, transparent information, the application of appropriate mechanisms, accountably practices, and the establishment of an independent supervisory institution. By establishing a reliable framework as such, those values are able to deliver positive-sum outcomes.

4. Producing a coherently theorised regulatory framework and rule for Formosan data protection law regime

The European data protection model is the most influentially global regulatory trend. It is recalled that the European data protection model roughly matches the PGC requirements, in ignorance of the PGC as the supreme moral principle. Some of the interpretations of the ECHR are problematic on the basis of the PGC-based value. However, it has been argued that the PGC remains valid. In this regard, the European data protection regime provides a substantial case study of reference for other data protection regimes. In pursuit of the purpose of producing an appropriate framework and rule for Formosan data protection law regime with respect to technologies at issue, I examined the analytic comparison of regulatory positions between European and Taiwanese situations in **Chapter 8**.

It is observed that the objectives and principles of data protection are similar in both areas, as the Formosan data protection law regime absorbs elements from (indeed, follows) the European data protection model. With this in mind, European countries and Taiwan share a high level of equivalent protection of personal data by having a main regulatory (or, ‘burdensome’) provision. Although there are differing

opinions and objections as to the acceptance of the European data protection model, I argued that there is a need to re-affirm the European model in the Formosan data protection regime. This is because the two rights and interests are simply not a zero-sum trade-off and conflict can be frequently and effectively avoided through valid consent. Moreover, even if there is a conflict, the criterion provided by PGC can be used to solve the problem.

As regards the differences, I examined three themes, namely, consent and public interests, the operation of data protection principles in effect, and the supervisory authorities. In the Formosan legal regime, the traditional value of ‘sacrificing oneself for the sake of the whole’ results in a worship of overvaluing public/ collective interest. Such a worship of public interest considerably diminished the role of consent and the effectiveness of operation of data protection principles. More importantly, there is no single independent supervisory authority in charge of data protection business.

The first suggestion relies on the attempts to apply the co-operative model to the legislation and their applications. First, a broad concept of privacy is fundamental to the suggested regulatory model. In this case, recent Constitutional Interpretations can be seen as an encouraging starting point. Secondly, on the basis of the principle of the priority of consent, I argued that where possible and practicable, valid consent should be obtained from each agent (data subject) prior to the collection, processing and use of personal data. In this respect, conditions of best practice have been attached in section 8.3.1. Thirdly, mechanisms such as PIA and PETs for establishing trust in agents should be encouraged to imply in the early stage. In this regard, supplementary measures to promote these mechanisms such as further education, concrete requirements in the legislation, good practices, public engagement, and to regard

investments in improving trustworthiness as regular investments, are strongly recommended. Lastly, in terms of the consideration on balancing interests and rights at issue, the worship, or illusion, of public interest including the ‘research interest’ must be put right. It is, again, recalled that technologies are not always stable, in particularly developing ones. A precautionary analysis thus is suggested to prevent generic harm. After all, on the basis of the PGC ground, what should be borne in mind is that the agents (or, individuals here) are the ultimate respondents of the generic rights.

Unlike the first suggestion which dealt with legislation and rules roughly in line with the European data protection model, the second suggestion concentrated on the institutional framework which has not yet been applied. In this case I have observed that the Formosan hydra-headed bureaucratic model generates inconsistent data protection implications. Moreover, without an appropriate level of independence and expertise, it seems unconvincing that relevant authorities are capable and credible to be in charge of data protection and privacy issues with respect to ICT in an information society. With this in mind, I have suggested that an institutional framework constituting an independent body with adequate advisory board, budgets, functions, powers and practice should be instituted to assist the success of the co-operative model. In sum, minor corrections to improve trustworthiness of data processing are encouraged; in particular a consistent approach to maintain valid consent, precautionary and preventive measures against risks of developing such technologies, and an independent institutional framework.

9.2 Future Research

Until now, I hope to have at least provided a defensible/ adequate theoretical framework and developed appropriate principles and guidelines in this field. The frequent situations occurring in daily life which inspired this thesis has never played a less primary role. Indeed, the technologies at issue have developed in a way that can be used in extensive applications in a considerably broad range of diverse environments. Accordingly, the right to benefit from advances of science and technology seems to be more crucial than ever. However, so do our concerns over privacy and data protection. This is particularly true with respect to new trends on biometric technologies in conjunction with remote RFID technology without the need of cooperation required from data subjects. Nevertheless, as Brownsword remarked in a lecture, 'in the information society there is never a shortage of critics with respect to privacy and data protection rights and informed consent.'[9] In this regard, what we need to do is to consistently and continually promote the generic conditions without harming, or diminishing the opportunities for agents to be entitled attempts to consent.

At least two plausible avenues of research in this regard can be envisaged.

First, we must not forget that there remains a gap between rapid technologies and regulations. It has been recalled by the WP29 that new trends on biometrics change their focus to profiling specific needs of individuals allowing more than merely identification or categorisation of an individual.[10] Crucially, the image of personal bodily integrity of an individual may soon be a complete picture in the eyes of data controllers. Although I have tried to provide some guidance, associated regulatory policies should always be assessed throughout the procedure of personal data

[9] Roger Brownsword, 'Informed Consent in the Information Society' (Durham CELLS Lecture, Durham, 8 May 2012).
[10] Article 29 Data Protection Working Party, *Opinion 3/2012 on Developments in Biometric Technologies* (No 00720/12/EN, WP193, 2012) 16-17.

collection and processing. In this regard, the operationalizing of the enhancement of the co-operative model will need, and will surely be inspired by, new technologies and technical/ social mechanisms. Consequently, updated research examining such objects on the basis of a broad concept of privacy can offer fertile ground for future study.

The second avenue for further research concerns reforms of data protection legal regimes. In the EU, a General Regulation of Data Protection has been drafted. Although the road to the completion of this stage of reform remains rather lengthy, it has at least arrived to a consistent confirmation of the European data protection approach. What we need to do is to closely assess its development as well as influences. As regards Formosan data protection law regime, on the other hand, it seems to me that, there are still many things to be improved. With this in mind, I consider that, on the basis of the principle of priority of consent, the starting point should be the more detailed clarification of the integrity of consent within data protection law.[11] Furthermore, an adequate institutional framework in charge of data protection and privacy should be continually encouraged in Taiwan.

[11] Section 6.4.1.

Biblography

Book

1. Akandji-Kombe J-F, *Positive obligations under the European Convention on Human Rights: A guide to the implementation of the European Convention on Human Rights* (Council of Europe 2007).
2. Axelrod R, *The Evolution of Cooperation* (Basic Books 1984).
3. ——, *The Complexity of Cooperation: Agent-Based Models of Competition and Collaboration* (Princeton University Press 1997).
4. Ayres I and Braithwaite J, *Responsive Regulation* (OUP 1992).
5. Baird D, Gertner R and Picker R, Game Theory and the Law (Harvard University Press 1994).
6. Bates B, *A Guide to Physical Examination and History Taking* (5th edn, Lippincott Williams and Wilkins 1991).
7. Bennett C and Raab C, *The Governance of Privacy: Policy Instruments in Global Perspective* (MIT Press 2006).
8. Bentham J, *An Introduction to the Principles of Morals and Legislation* (Burns JH and Hart HLA eds, 1970).
9. Beyleveld D and Brownsword R, *Law as a Moral Judgement* (Sweet and Maxwell 1986).
10. ——, *Human Dignity in Bioethics and Biolaw* (OUP 2001).
11. ——, *Consent in the Law* (Hart Publishing 2007).
12. Beyleveld D, *The Dialectical Necessity of Morality: An Analysis and Defence of Alan Gewirth's Argument to the Principle of Generic Consistency* (The University of Chicago Press 1991).
13. Bielby P, *Competence and Vulnerability in Biomedical Research* (Springer 2008)
14. Boylan M, *Gewirth: Critical Essays on Action, Rationality, and Community* (Rowman & Littlefield 1999).
15. Brownsword R, *Rights, Regulation, and the Technological Revolution* (OUP 2008).
16. Bygrave LA, *Data Proteciton Law: Approaching Its Rationale, Logic and Limits* (Kluwer Law International 2002).

17. Carey P, *Data Protection: A Practical Guide to UK and EU Law* (2nd edn, OUP 2004).
18. Cassese A, *International Law* (2nd edn, OUP 2005).
19. Chen H, *Medical Genetic Handbooks* (MO: W.H. Green 1998).
20. Collingridge D, *The Social Control of Technology* (Palgrave Macmillan 1981).
21. Craig P and Búrca GD, *EU Law: Text, Cases and Materials* (5th edn, OUP 2011).
22. DeCew J, *In Pursuit of Privacy: Law, Ethics, and the Rise of Technology* (Cornell University Press 1997).
23. Delany H and Carolan E, *The Right to Privacy: A Doctrinal and Comparative Analysis* (Thomson Round Hall 2008).
24. Duda RO and Hart PE, *Classification and Scene Analysis* (John Wiley & Sons, Inc. 1973).
25. Dworkin R, *Taking Rights Seriosly* (New impression with a reply to critics, Duckworth 2005).
26. Etzioni A, *The Limits of Privacy* (Basic Books 1999).
27. Feldman D, *Civil Liberties and Human Rights in England and Wales* (2nd edn, OUP 2002).
28. Fenwick H, *Civil Liberties and Human Rights* (4th edn, Routledge-Cavendish 2007)0
29. Freeman MDA, *Lloyd's Introduction to Jurisprudence* (8th edn, Sweet & Maxwell 2008).
30. Fukuyama F, *Our Posthuman Future* (Profile Books 2002)0
31. Garfinkel S, *Database Nation : The Death of Privacy in the 21st Century* (O'Reilly Media 2001).
32. Gauthier D, *Morals by Agreement* (OUP 1986).
33. Gewirth A, *Reason and Morality* (University of Chicago Press 1978).
34. ——, *The Community of Rights* (The University of Chicago Press 1996).
35. Gunningham N and Grabosky P, *Smart Regulation* (Claredon Press 1998).
36. Hare RM, *Moral Thinking: Its Levels, Methods and Point* (OUP 1982).
37. Harris D and others, *Harris, O'Boyle & Warbrick: Law of the European Convention on Human Rights* (2nd edn, OUP 2009).
38. Heisenberg D, *Negotiating Privacy: The European Union, The United States, and Personal Data Protection* (Lynne Rienner Publisher 2005).
39. Himmelfarb G, *On Liberty and Liberalism: The Case of John Stuart Mill* (Alfred A. Knopf 1974).

40. Inness J, *Privacy, Intimacy, and Isolation* (OUP USA 1992).
41. International Organization for Migration, *Biometrics and International Migration* (International Organization for Migration 2005).
42. Karanja SK, *Transparency and Proportionality in the Schengen Information System and Border Control Co-operation* (Martinus Nijhoff Publishers 2008).
43. Kholmatov A, *Privacy Protecting Biometric Authentication Systems – A Novel Framework to Protect Privacy* (VDM Verlag 2009).
44. Laurie G, Genetic Privacy: A Challenge to Medico-Legal Norms (CUP 2002).
45. Leigh I and Masterman R, *Making Rights Real: The Human Rights Act in its First Decade* (Hart Publishing 2008).
46. Letsas G, *A Theory of Interpretation of the European Convention on Human Rights* (OUP 2007).
47. Manson NC and O'Neill O, *Rethinking Informed Consent in Bioethics* (CUP 2007).
48. Mason K and Laurie G, *Mason and McCall Smith's Law and Medical Ethics* (8th edn, OUP 2011).
49. Mill JS, *On Liberty* (first published 1859, Batoche Books 2001).
50. ——, *Utilitarianism* (Sher G ed, first published 1861, Hackett publishing 1979).
51. Mills JL, *Privacy: the Lost Right* (OUP 2008).
52. Mowbray A, *The Development of Positive Obligations under the European Convention on Human Rights by the European Court of Human Rights* (Hart Publishing 2004).
53. Nanavati S, Thieme M and Nanavati R, *Biometrics: Identity Verification in a Networked World – A Wiley Tech Brief* (John Wiley & Sons, Inc. 2002).
54. Nozick R, *Anarchy, State, and Utopia* (Blackwell 1974).
55. Nuffield Council on Bioethics, *Genetically Modified Crops: The Ethical and Social Issues* (Nuffield Council on Bioethics, 1999).
56. Pattinson SD, *Influencing Traits Before Birth* (Ashgate Publishing 2002).
57. ——, *Medical Law and Ethics* (2nd edn, Sweet & Maxwell Limited 2009).
58. Posner EA and Vermeule A, *Terror in the Balance: Security, Liberty and the Courts* (OUP 2007).
59. Posner RA, *Economic Analysis of Law* (5th edn, Aspen Publishers 1998).
60. ——, *The Economics of Justice* (Harvard University Press 1981).
61. Rawls J, *A Theory of Justice* (Revised edn, Belknap Press of Harvard University Press 1999).

62. ——, *Political Liberalism: Expanded Edition* (2nd edn, Columbia University Press 2005).
63. Rosen J, *The Naked Crowd: Reclaiming Security and Freedom in an Anxious Age* (Random House 2004).
64. Rössler B, *The value of privacy* (Polity Press 2005).
65. Sandel MJ, *Justice: What's the Right Thing to Do* (Penguin Books 2010).
66. Shackleton AJ, *Formosa Calling: An Eyewitness Account of the February 28th 77947 Incident* (The Taiwan Publishing Co. 1998).
67. Solove DJ and Schwartz PM, *Informational Privacy Law* (3 edn, Aspen Publishers 2009).
68. Solove DJ, *Nothing to Hide: the False Tradeoff between Privacy and Security* (Yale University Press 2011).
69. ——, *Understanding Privacy* (Harvard University Press 2009).
70. The Irish Council for Biometrics, *Biometrics: Enhancing Security or Invading Privacy? Opinion* (The Irish Council for Biometrics 2009).
71. Turpin C and Tomkins A, *British Government and the Constitution* (6th edn, CUP 2007).
72. White R and Ovey C, *Jacobs, White and Ovey, The European Convention on Human Rights* (5th edn, OUP 2010).
73. Williams B, *Ethics and the Limits of Philosophy* (Taylor & Francis 2006).
74. Woodward JD and others, *Army Biometric Applications: Identifying and Addressing Sociocultural Concerns* (RAND Publications 2001).
75. Woodward JD, Orlans NM and Higgins PT, *Biometrics: Identity Assurance in the Information Age* (McGraw-Hill 2003).
76. Zweigert K and Kötz H, *An Introduction to Comparative Law* (Weir T tr, 3rd edn, OUP 1998).

Conference Paper

1. Beyleveld D, ‘Is consent necessary and/ or sufficient to authorise medical database research?’ (Regulation and Governance of Medical Database Research in the United Kingdom, Sheffield, 17th June 2011).

2. Brownsword R, ‘Informed Consent in the Information Society’ (Durham CELLS Lecture, Durham, 8 May 2012).
3. Marks S, ‘Out of Obsecurity: the Right to Benefit from Advances in Science and Technology and Its Implications for Global Health’ (The 3rd conference on Law, Science, and Technology: Health, Science, and Human Rights, Taipei, 18 December 2010).
4. Matsumoto T, ‘Importance of Open Discussion on Adversarial Analyses for Mobile Security Technologies, International Telecommunication Union’ (Telecommunication Standardization Sector, International Telecommunication Union Workshop on Security).

Contribution to an Edited Book

1. Barendt E, ‘Ptivacy as a Constitutional Right and Value’ in Birks P (ed), *Privacy and Loyalty* (Claredon Press 1997).
2. Benn SI, ‘Freedom, and Respect for Persons’ in Pennock JR and Chapman JW (eds), *Nomos XIII: Privacy* (Atherton Press 1971)
3. Beyleveld D and Brownsword R, ‘Complex Technology, Complex Calculations: Uses and Abuses of Precautionary Reasoning in Law’ in Sollie P and Düwell M (eds), *Evaluating New Technologies* (Springer 2009).
4. Beyleveld D and Pattinson SD, ‘Confidentiality and Data Protection’ in Grubb A, Laing J and McHale J (eds), *Principles of Medical Law* (3rd edn, OUP 2010).
5. Beyleveld D and Pattinson SD, ‘Individual Rights, Social Justice, and the Allocation Of Advances in Biotechnology’ in Boylan M (ed), *Public Health Policy and Ethics* (Kluwer 2004).
6. Beyleveld D and Pattinson SD, ‘Moral Interests, Privacy, and Medical Research’ in Boylan M (ed), *International Public Health Policy and Ethics* (Springer Netherlands 2008).
7. Beyleveld D, ‘An Overview of Directive 95/46/EC in Relation to Medical Research’ in Beyleveld D and others (eds), *The Data Protection Directive and Medicial Research Across Europe* (Ashgete Publishing 2004).
8. Beyleveld D, ‘Conceptualising Privacy in Relation to Medical Research Values’ in

9. Beyleveld D, ‘The Duty to Provide Informaiton to the Data Subject: Articles 10 and 11 of Directive 95/46/EC’ in Beyleveld D and others (eds), *The Data Protection Directive and Medicial Research Across Europe* (Ashgate Publishing 2004).
10. Blarkom GWv, Borking JJ and Verhaar P, ‘PET’ in Blarkom GWv, Borking JJ and Olk JGE (eds), *Handbook of Privacy and Privacy-Enhancing Technologies - The case of Intelligent Software Agents* (College bescherming persoonsgegevens 2003).
11. Borking JJ, ‘Why Adopting Privacy Enhancing Technologies (PETs) Takes so Much Time’ in Gutwirth S and others (eds), *Computers, Privacy and Data Protection: an Element of Choice* (Springer 2011).
12. Brownsword R, ‘Consent in Data Protection Law: Privacy, Fair Processing and Confidentiality’ in Gutwirth S and others (eds), *Reinventing Data Protection?* (Springer 2009).
13. Brownsword R, ‘So What Does the World Need Now? Reflections on Regulating Technologies’ in Brownsword R and Yeung K (eds), *Regulating Technologies: Legal Futures, Regulatory Frames and Technological Fixes* (Hart Publishing 2008).
14. Burkert H, ‘Privacy-Enhancing Technologies: Typology, Critique, Vision’ in Agre PE and Rotenberg M (eds), *Technology and Privacy: The New Landscape* (MIT Press 1998).
15. Chang W-C, ‘Transnational Constitutional Dialogues: An Empirical Study on Foreign Law Citations by the Constitutional Court of Taiwan’ in Hwang S-P (ed), *Constitutional Interpretation: Theory and Practice Vol 7 Part Il* (Institutum Iurisprudentiae, Academia Sinica 2010).
16. Craig P, ‘Unreasonableness and Proportionality in UK Law’ in Ellis E (ed), *The Principle of Proportionality in the Laws of Europe* (Hart Publishing 1999).
17. Dannemann G, ‘Comparative Law: Study of Similarities or Differences?’ in Reimann M and Zimmermann R (eds), *The Oxford Handbook of Comparative Law* (OUP 2006).
18. Feldman D, ‘Proportionality and the Human Rights Act 1998’ in Ellis E (ed), *The Principle of Proportionality in the Laws of Europe* (Hart Publishing 1999).
19. Garlicki L, ‘The European Court of Human Rights and the "Margin of Appreciation" Doctrine: How much Discretion is Left to a State in Human Rights Matters?’ in Huang C-Y (ed), *Administrative Regulation and Judicial Remedies 2010* (Institutum Iurisprudentiae, Academia Sinica 2011).

20. Guagnin D, Hempl L and Ilten C, ‘Privacy Practices and the Claim for Accountability’ in Schomberg Rv (ed), *Towards Responsible Research and Innovation in the Information and Communication Technologies and Security Technologies Fields* (Publications Office of the European Union 2011).
21. Gürses S and Berendt B, ‘PETs in the Surveillance Society: A Critical Review of the Potentials and Limitations of the Privacy as Confidentiality Paradigm’ in Gutwirth S, Poullet Y and Hert PD (eds), *Data Protection in a Profiled World* (Springer 2010).
22. Hare RM, ‘Do Agents Have to Be Moralists?’ in Edward Regis J (ed), *Gewirth's Ethical Rationalism: Critical Essays with a Reply by Alan Gewirth* (University of Chicago Press 1984).
23. Hartlev M, ‘The Concept of Privacy: An Analysis of the EU Directive on the Protection of Personal Data’ in Beyleveld D and others (eds), *The Data Protection Directive and Medicial Research Across Europe* (Ashgete Publishing 2004).
24. Jain A, Bolle R and Pankanti S, ‘Introduction to Biometrics’ in Jain A, Bolle R and Pankanti S (eds), *Biometrics: Personal Identification in Networked Society* (Kluwer Academic Publishers 1999).
25. Jansen N, ‘Comparative Law and Comparative Knowledge’ in Reimann M and Zimmermann R (eds), *The Oxford Handbook of Comparative Law* (OUP 2006).
26. Juels A, ‘RFID Privacy: A Technical Primer for the Non-Technical Reader’ in Strandburg KJ and Raicu DS (eds), *Privacy and technologies of identity: a cross-disciplinary conversation* (Springer 2006).
27. Korba L, Patrick A and Song R, ‘Trust model and network aspects’ in Blarkom GWv, Borking JJ and Olk JGE (eds), *Handbook of Privacy and Privacy-Enhancing Technologies - The case of Intelligent Software Agents* (College bescherming persoonsgegevens 2003).
28. Leenes R, Koops B-J and Hert Pd, ‘Introduction’ in Leenes R and others (eds), *Constitutional rights and new technologies: a comparative study* (T.M.C.Asser Press 2008).
29. Leigh I, ‘Concluding Remarks’ in Fenwick H, Phillipson G and Masterman R (eds), *Judicial Reasoning under the UK Human RIghts Act* (CUP 2007).
30. Liao F-T and Weng Y-H, ‘Dilemma or Co-existence: Collecting Individual Information and Protection of Information Privacy’ in The Editing Committee on Celebrating the Seventieth Birthday of Professor Chung-Mo Cheng (ed), *Issues on Public Law in the 21st Century* (New Sharing Publishing 2008).

31. Lin T-Y, ‘Genetic Information and Genetic Privacy: the Processing and Legislative Framework of Genetic Information from the Perspective of Protecting the Right to Privacy’ in The Editing Committee on Celebrating the Seventieth Birthday of Professor Yueh-Sheng Weng (ed), *Contemporary Public Law Issues*, vol 2 (Angel Publisher 2002).
32. Lord Hoffmann, ‘The Influence of the European Principle of Proportionality upon UK Law’ in Ellis E (ed), *The Principle of Proportionality in the Laws of Europe* (Hart Publishing 1999).
33. Masterman R, ‘Aspiration or Foundation? Tha Status of the Strasbourg Jurisprudence and the 'Convention Rights' in Domestic Law’ in Fenwick H, Phillipson G and Masterman R (eds), *Judicial Reasoning under the UK Human RIghts Act* (Cambridge University Press 2007).
34. McBride J, ‘Proportionality and the European Convention on Human Rights’ in Ellis E (ed), *The Principle of Proportionality in the Laws of Europe* (Hart Publishing 1999).
35. Menevidis Z, Swartzman S and Stylianidis E, ‘Code of Conduct for FP7 Researchers on Medical and Biometric Data Privacy’ in Schomberg Rv (ed), *Towards Responsible Research and Innovation in the Information and Communication Technologies and Security Technologies Fields* (Publications Office of the European Union 2011).
36. Michaels R, ‘The Functional Method of Comparative Law’ in Reimann M and Zimmermann R (eds), *The Oxford Handbook of Comparative Law* (OUP 2006).
37. Mordini E, ‘ANNEX I: Policy Brief on: Whole Body – Imaging at Airport Checkpoints: the Ethical and Policy Context’ in Schomberg Rv (ed), *Towards Responsible Research and Innovation in the Information and Communication Technologies and Security Technologies Fields* (Towards Responsible Research and Innovation in the Information and Communication Technologies and Security Technologies Fields 2011).
38. Nouwt S, ‘Towards a Common European Approach to Data Protection: A Critical Analysis of Data Protection Perspectives of the Council of Europe and the European Union’ in Gutwith S and others (eds), *Reinventing Data Protection?* (Springer 2009).
39. Peissl W, ‘Responsible Research and Innovation in ICT: The Case of Privacy’ in Schomberg Rv (ed), *Towards Responsible Research and Innovation in the Information and Communication Technologies and Security Technologies Fields* (Publications Office of the European Union 2011).
40. Beyleveld D and Pattinson SD, ‘Precautionary Reasoning as a Link to Moral Action’

in Michael B (ed), *Medical Ethics* (Prentice-Hall 2000).

41. Phillipson G, 'Clarity Postponed: Horizontal Effect after Campbell' in Fenwick H, Phillipson G and Masterman R (eds), *Judicial Reasoning under the UK Human RIghts Act* (Canbridge University Press 2007).
42. Poullet Y, 'About the E-Privacy Directive: Towards a Third Generation of Data Protection Legislation?' in Gutwirth S, Poullet Y and Hert PD (eds), *Data Protection in a Profiled World* (Springer 2010).
43. Putnam RA, 'Why Not a Feminist Theory of Justice?' in Nussbaum MC and Glover J (eds), *Women, Culture and Development: A Study of Human Capabilities* (OUP 1995).
44. Rejman-Greene M, 'Privacy Issues in the Application of Biometrics: a European Perspective' in Wayman JL and others (eds), *Biometric Systems: Technology, Design and Performance Evaluation* (Springer 2005).
45. Rouillé-Mirza S and Wright J, 'Comparative Study on the Implementation and Effect of Directive 95/46/EC on Data Protection in Europe: Medical Research' in Beyleveld D and others (eds), *Data Protection Directive and Medicial Research Across Europe* (Ashgate Publishing 2004).
46. Schomberg Rv, 'Introduction: Towards Responsible Research and Innovation in the Information and Communication Technologies and Security Technologies Fields' in Schomberg Rv (ed), *Towards Responsible Research and Innovation in the Information and Communication Technologies and Security Technologies Fields* (Publications Office of the European Union 2011).
47. Schwartz PM, 'Privacy Inalienability and Personal Data Chips' in Strandburg KJ and Raicu DS (eds), *Privacy and technologies of identity: a cross-disciplinary conversation* (Springer 2006).
48. Sethi IK, 'Biometrics: Overview and Applications' in Strandburg KJ and Raicu DS (eds), *Privacy and Technologies of Identity: A Cross-disciplinary Conversation* (Springer 2006).
49. Smith S, 'Precautionary Reasoning in Determining Moral Worth' in Freeman M (ed), Law and Bioethics: Current Legal Issues Volume 11 (OUP 2008).
50. Stahl BC, 'IT for a Better Future. How to Integrate Ethics, Politics and Innovation' in Schomberg Rv (ed), *Towards Responsible Research and Innovation in the Information and Communication Technologies and Security Technologies Fields* (Publications Office of the European Union 2011).
51. Vries Kd 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 2011).

52. Wayman JL and others, 'An Introduction to Biometric Authentication Systems' in Wayman JL and others (eds), *Biometric Systems: Technology, Design and Performance Evaluation* (Springer 2005).
53. Wei G and Li D, 'Biometrics: Applications, Challenges and the Future' in Strandburg KJ and Raicu DS (eds), *Privacy and Technologies of Identity: A Cross-disciplinary Conversation* (Springer 2006).
54. Wright D and others, 'Precaution and Privacy Impact Assessment as Modes towards Risk Governance' in Schomberg Rv (ed), *Towards Responsible Research and Innovation in the Information and Communication Technologies and Security Technologies Fields* (Publications Office of the European Union 2011).

Edited Book

1. Edward Regis J (ed) *Gewirth's Ethical Rationalism: Critical Essays with a Reply by Alan Gewirth* (University of Chicago Press 1984).

Eletronic Article

1. Allen A, 'Privacy and Medicine' The Stanford Encyclopedia of Philosophy <http://plato.stanford.edu/archives/sum2009/entries/privacy-medicine/> accessed 21 February 2011.
2. DeCew J, 'Privacy' The Stanford Encyclopedia of Philosophy <http://plato.stanford.edu/archives/fall2008/entries/privacy/> accessed 21 Feburary 2011.
3. Department of Constitutional Affairs, 'Proposals for Amendment made by Austria, Finland, Sweden and the United Kingdom: Explanatory Note' <http://www.dca.gov.uk/ccpd/dpdamend.htm> accessed 18 January 2010.

4. Hert Pd, ‘Biometrics at the Frontiers: Assessing the Impact on Society’ <http://cybersecurity.jrc.ec.europa.eu/docs/LIBE%20Biometrics%20March%2005/iptsBiometics_FullReport_eur21585en.pdf> accessed 29 July 2010.
5. ——, ‘Biometrics: legal Issues and Implications’ Background paper for the Institute of Prospective Technological Studies, DG JRC – Sevilla, European Commission <https://public.univie.ac.at/fileadmin/user_upload/inst_staatswissenschaften/Frisch/21063courseWebsite/LegalImplications_Paul_de_Hert.pdf> accessed 9 November 2011.
6. Hornung G, ‘The European Regulation on Biometric Passports: Legislative Procedures, Political Interactions, Legal Framework and Technical Safeguards’ SCRIPT-ed <http://www.law.ed.ac.uk/ahrc/SCRIPT-ed/vol4-3/hornung.asp> accessed 18 November 2009.
7. Information Commissioner Office, ‘Data Protection Technical Guidance: Radio Frequency Identification’ <http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/radio_frequency_indentification_tech_guidance.pdf> accessed 18 November 2009.
8. ——, ‘The Use of Biometrics in Schools’ <http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/fingerprinting_final_view_v1.11.pdf> accessed 18 November 2009.
9. Kuhn S, ‘Prisoner's Dilemma’ The Stanford Encyclopedia of Philosophy <http://plato.stanford.edu/entries/prisoner-dilemma/> accessed 5 May 2012.
10. Maghiros I and others, ‘Biometrics at the Frontiers: Assessing the Impact on Society’ <http://cybersecurity.jrc.ec.europa.eu/docs/LIBE%20Biometrics%20March%2005/iptsBiometics_FullReport_eur21585en.pdf> accessed 29 July 2010.
11. Ross D, ‘Game Theory’ The Stanford Encyclopedia of Philosophy <http://plato.stanford.edu/entries/game-theory/> accessed 5 May 2012.
12. UNESCO, ‘The Right to Enjoy the Benefits of Scientific Progress and its Applications’ <http://unesdoc.unesco.org/images/0018/001855/185558e.pdf> accessed 3 August 2011.
13. Verbeek B, ‘Game Theory and Ethics’ The Stanford Encyclopedia of Philosophy <http://plato.stanford.edu/entries/game-ethics/> accessed 5 May 2012.

Journal Article

1. Aleinikoff TA, ‘Constitutional Law in the Age of Balancing’ 96 Yale Law Journal 943-1005.
2. Alexy R, ‘Effects of Defects—Action or Argument? Thoughts about Deryck Beyleveld and Roger Brownsword’s Law as a Moral Judgment’ 19 Ratio Juris 169-179.
3. ——, ‘On the Concept and the Nature of Law’ 21 Ratio Juris 281-299.
4. ——, ‘The Dual Nature of Law’ 23 Ratio Juris 167-182.
5. Allen A, ‘Coercing Privacy’ 40 William and Mary Law Review 723-757.
6. ——, ‘Taking Liberties: Privacy, Private Choice, and Social Contract Theory.’ (1987) 56 Cincinnate Law Review 461-492.
7. Beyleveld D and Bos G, ‘The Foundational Role of the Principle of Instrumental Reason in Gerwirth's Argument for the Principle of Generic Consistency: A Response to Andrew Chitty’ 20 King's Law Journal 1-20.
8. Beyleveld D and Brownsword R, ‘My Body, My Body Parts, My Property?’ (2000) 8 Health Care Analysis 87-99.
9. ——, ‘Principle, Proceduralism, and Precaution in a Community of Rights’ 19 Ratio Juris 141-168.
10. Beyleveld D and Pattinson SD, ‘Defending Moral Precaution as a Solution to the Problem of Other Minds: A Reply to Holm and Coggon’ 23 Ratio Juris 258-273.
11. Beyleveld D, ‘A Reply to Marcus G. Singer on Gewirth, Beyleveld and Dialectical Necessity’ (2002) 15 Ratio Juris 458-473.
12. ——, ‘Data Protection and Genetics: Medical Research and the Public Good’ 18 King's Law Journal 275-289.
13. ——, ‘Legal Theory and Dialectically Contingent Justifications for the Principle of Generic Consistency’ (1996) 9 Ratio Juris 15-41.
14. ——, ‘The Principle of Generic Consistency as the Supreme Principle of Human Rights’ (2012) 13 Human Rights Review 1-18.
15. Bignami F, ‘Privacy and Law Enforcement in the European Union: The Data Retention Directive’ (2007) 8 Chicago Journal of International Law 233-256.
16. ——, ‘Transgovernmental Networks vs. Democracy: The case of the European Information Privacy Network’ 26 MICH J INT’L L 807-868.
17. Blume P, ‘Transbroder Data Flow: Is There a Solution in Sight?’ (2000) 8

International Journal of Law and Information Technology 65-86.
18. Bond E, ‘Gewirth on Reason and Morality’ (1980) 11 Metaphilosopy 36-53.
19. Brandt R, ‘The Future of Ethics’ (1981) 15 Nous 31-40.
20. Brown R, ‘Rethinking Privacy: Exclusivity, Private Relation and Tort Law’ (2006) 43 Alberta Law Review 589-614.
21. Brownsword R, ‘The Cult of Consent: Fixation and Fallacy’ (2004) 15 King's Law Journal 223-252.
22. Busby H, Hervey TK and Mohr A, ‘Ethical EU Law? The Influence of the European Group on Ethics’ (2008) 33 E.L. REV. 803-842.
23. Chang W-C, ‘The Role of Judicial Review in Consolidating Democracy: the Case of Taiwan’ (2005) 2 Asia Law Review 73-88.
24. Chen C-L, ‘In Search of a New Approach of Information Privacy Judicial Review: Interpreting No. 603 of Taiwan's Constitutional Court as a Guide’ (2010) 20 Indiana International and Comparative Law Review 21-46.
25. Chiou W-T, ‘Comments on the Framework Problems of the Draft of Computer-Processed Personal Data Protection Law from the Perspective of the Conceptual Distinction between Information Self-determination and Information Privacy’ (2009) 168 The Taiwan Law Review 172-189. (in Chinese)
26. Chitty A, ‘Protagonist and Subject in Gewirth's Argument for Human Rights’ 19 King's Law Journal 1-26.
27. Clucas B, ‘The Sheffield School and Discourse Theory: Divergences and Similarities in Legal Idealism/Anti-Positivism’ 19 Ratio Juris 230-244.
28. Costa L, ‘Privacy and the Precautionary Principle’ (2012) 28 Computer Law & Security Review 14-24.
29. Craig P, ‘Once upon a Time in the West: Directive Effect and the Federalization of EEC Law’ 12 Oxford Journal of Legal Studies 453-479.
30. Fenwick H and Phillipson G, ‘Confidence and Privacy: A Re-examination’ (1996) 55 Cambridge Law Journal 447-455.
31. Fried C, ‘Natural Law and the Concept of Justice’ 74 Ethics 237-254.
32. ——, ‘Privacy’ 77 Yale Law Journal 475-493.
33. Gerety T, ‘Redefining Privacy’ (1977) 12 Harvard Civil Rights-Civil Liberties Law Review 233-296.
34. Gewirth A, ‘The Basis and Content of Human Rights’ (1979) 13 Georgia Law Review 1143-1170.

35. Haddow G and others, ‘'Nothing Is Really Safe': A Focus Group Study on the Processes of Anonymizing and Sharing of Health Data for Research Purposes’ (2011) 17 Journal of Evaluation in Clinical Practice 1140-1146.
36. Hall JAY and Kimura D, ‘Dermatoglyphic Asymmetry and Sexual Orientation in Men’ (1994) 108 Behavioral Neuroscience 1203-1206.
37. Harman G, ‘Justice and Moral Bargaining’ (1983) 1 Social Philosophy and Policy 114-131.
38. Hoepman J-H and others, ‘Crossing Borders: Security and Privacy Issues of the European e-Passport’ (2006) 4266 Lecture Notes in Computer Science 152-167.
39. Holm S and Coggon J, ‘A Cautionary Note against “Precautionary Reasoning” in Action Guiding Morality ’ 22 Ratio Juris 295-309.
40. Howard R, ‘The Full-Belly Thesis: Should Economic Rights Take Priority over Civil and Political Rights? Evidence from Sub-Saharan Africa’ (1983) 5 Human Rights Quarterly 467-490.
41. Koller P, ‘The Concept of Law and Its Conceptions’ 19 Ratio Juris 180-196.
42. Kong L, ‘Enacting China's Data Protection Act’ (2010) 18 International Journal of Law and Information Technology 197-266.
43. Koops B-J and Leenes R, ‘'Code' and the Slow Erosion of Privacy’ 12 Michigan Telecommunications and Technology Law Review 115-188.
44. Lee C-L, ‘The Conflict and Balance between the Freedom of Media and the Protection of Private Life: Brief Comments on J. Y. Interpretation No. 689’ (2011) 184 The Taiwan Law Review 29-49. (in Chinese)
45. Liberatore A, ‘Balancing Security and Democracy, and the Role of Expertise: Biometrics Politics in the European Union’ (2007) 13 Eur J Crim Policy Res 109-137.
46. Liu C-Y, ‘Not So Improved: Initial Commentry on the Personal Data Protection Law’ (2010) 183 The Taiwan Law Review 147-164. (in Chinese)
47. Liu Y, ‘Identifying Legal Concerns in the Biometric Context’ 3: 1 Journal of International Commercial Law and Technology 45-54.
48. ——, ‘The Principle of Proportionality in Biometrics: Cases Studies from Norway’ 25 Computer Law & Security Review 237-250.
49. Lu D-W, ‘Brief Commentary on the Amendment of Personal Data Protection Law’ (2010) 183 The Taiwan Law Review 131-146. (in Chinese)
50. Mclean WHI, ‘Genetic Disorder of Palm Skin and Nail’ 202 Journal of Anatomy 133-141.

51. McMahon C, ‘Gewirth's Justification of Morality’ (1986) 50 Philosophical Studies 261-281.
52. Moore AD, ‘Owning Genetic Information and Gene Enhancement Techniques: Why Privacy and Property May Undermine Social Control of the Human Genome’ (2000) 14 Bioethics 97-119.
53. Moran L, ‘*Laskey v The United Kingdom*: Learning The Limits of Privacy’ 61 Mod L Rev 77-84.
54. Moreham NA, ‘The Right to Respect for Private Life in the European Convention on Human Rights: a Re-examination’ 1 EHRLR 44-79.
55. O'Gorman L, ‘Comparing Passwords, Tokens, and Biometrics for User Authentication’ 91 Proceedings of the IEEE 2019-2040.
56. Ohm P, ‘Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization’ (2010) 57 UCLA Law Review 1701-1777.
57. Orlikowski WJ, ‘Sociomaterial Practices: Exploring Technology at Work’ (2008) 28 Organization Studies 1435-1448.
58. Pattinson SD, ‘Directed Donation and Ownership of Human Organs’ (2011) 31 Legal Studies 392-410.
59. Peikoff AL, ‘The Right to Privacy: Contemporary Reductionists and Their Critics’ 13 Virginia Journal of Social Policy and the Law 474-551.
60. Peng S-Y, ‘Privacy and the Construction of Legal Meaning in Taiwan’ (2003) 37 The International Lawyer 1037-1054.
61. Phillipson G, ‘Transforming Breach of Confidence? Towards a Common Law Right of Privacy under the Human Rights Act’ (2003) 66 Mod L Rev 726-758.
62. Piris J-C, ‘The legal orders of the European Community and of the Member States: peculiarities and influences in drafting’ 58 Amicus Curiae 21-28.
63. Posner RA, ‘The Right of Privacy’ 12 Georgia Law Review 393-422.
64. Rachels J, ‘Why Privacy is Important’ 4 Philosophy and Public Affairs 323-333.
65. Reidenberg J, ‘Setting Standards for Fair Information Practice in the U.S. Private Sector’ 80 IOWA L REV 497-530.
66. Saunders C and others, ‘Asian Constitutions in Comparative Perspectives’ (2009) 4 National Taiwan University Law Review 187-214.
67. Schartum DW, ‘Designing and Formulating Data Protection Laws’ (2010) 1 International Journal of Law and Information Technology 1-27.
68. Scheuermann J, ‘Gewirth's Concept of Prudential Rights’ (1987) 37 Philosophical

69. Schoeman F, ‘Privacy: Philosophical Dimensions’ 21 American Philosophical Quarterly 199-213.
70. Schuster MM, ‘Gastroenterology: Fingerprinting gi disease’ April Johns Hopkins Physician Update 5.
71. Schwartz A, ‘Review of Reason and Morality, by Alan Gewirth’ (1979) 88 Philosophical Review 654-656.
72. Schwartz PM and Solove DJ, ‘The PII Problem: Privacy and A New Concept of Personally Identifiable Information’ (2011) 86 NYU Law Review 1814-1894.
73. Singer MG, ‘Gewirth, Beyleveld, and Dialectical Necessity’ (2000) 13 Ratio Juris 177-195.
74. Solove DJ, ‘"I've Got Nothing to Hide" and Other Misunderstandings of Privacy’ (2007) 44 San Diego Law Review 745-772.
75. ——, ‘Conceptualizing Privacy’ 90 California Law Review 1087-1154.
76. ——, ‘Privacy and Power: Computer Databases and Metaphors for Information Privacy’ (2001) 53 Stanford Law Review 1393-1462.
77. Sterba JP, ‘Justifying Morality: The Right and the Wrong Ways’ (1987) 72 Synthese 45-69.
78. Stewart R, ‘Reformation of American Administrative Law’ (1975) 88 Harvard Law Review 1667-1813.
79. Thomson JJ, ‘The Right to Privacy’ 4 Philosophy and Public Affairs 295-314.
80. Toddington S, ‘The Moral Truth about Discourse Theory’ 19 Ratio Juris 217-229.
81. Torre ML, ‘On Two Distinct and Opposing Versions of Natural Law: “Exclusive” versus “Inclusive”’ 19 Ratio Juris 197-216.
82. Wang M-L, ‘Information Privacy in a Network Society: Decision Making Amidst Constant Change’ (2010) 5 National Taiwan University Law Review 127-154.
83. Wang T-C, ‘The Issue and the Development of Protecting the Right to Personality (III): the Materialization of the Right to Personality and Its Scope’ (2007) 97 Taiwan Law Journal 27-50. (in Chinese)
84. Ward T, ‘Two Schools of Legal Idealism: A Positivist Introduction’ 19 Ratio Juris 127-140.
85. Warren A and others, ‘Privacy Impact Assessments: International Experience as a Basis for UK Guidance’ (2008) 24 Computer Law & Security Review 233-242.
86. Warren S and Brandeis L, ‘The Right to Privacy’ (1890) 14 Harvard Law Review

193-220.

87. Wickins J, ‘The Ethics of Biometrics: the Risk of Social Exclusion from the Widespread Use of Eletronic Identification’ (2007) 13 Sci Eng Ethics 45-54.

Newspaper Article

1. Banyan, ‘America’s Security Commitment to Taiwan: From Keystone to Millstone?’ *The Economist* (London, 3 March 2011) <http://www.economist.com/blogs/banyan/2011/03/america%E2%80%99s_security_commitment_taiwan> accessed 5 March 2011.
2. ——, ‘Taiwan's Commonsense Consensus: Economic Integration with China Is not Doing What China Hoped and the Opposition Feared’ *The Economist* (London, 24 February 2011) <http://www.economist.com/node/18229208> accessed 5th March, 2011.
3. BBC, ‘Theresa May: Numbers of Unchecked at UK Borders Unknown’ *BBC* (London, 7 November 2011) <http://www.bbc.co.uk/news/uk-politics-15615537> accessed 9 November 2011.
4. Bunting M, ‘Phone-hacking scandal is an outrage of human decency’ *The Guardian* (14 July 2011) <http://www.guardian.co.uk/commentisfree/2011/jul/14/phone-hacking-scandal-ethics> accessed 14 July 2011.
5. Loa I-s, ‘Groups Decry Revision of Data Act’ *Taipei Times* (Taipei, 29th April 2010) 3 <http://www.taipeitimes.com/News/taiwan/archives/2010/04/29/2003471758> accessed 22 March, 2011.

Report, Command Paper

1. Article 29 Data Protection Working Party, *Opinion 01/2012 on the Data Protection Reform Proposals* (No 00530/12/EN, WP191, 2012).
2. ——, *Opinion 02/2012 on Facial Recognition in Online and Mobile Services* (No 00727/12/EN, WP192, 2012).
3. ——, *Opinion 04/2012 on Cookie Consent Exemption* (No 00879/12/EN, WP194,

2012).

4. ——, *Opinion 15/2011 on the Definition of Consent* (01197/11/EN, WP187, 2011).
5. ——, *Opinion 3/2005 on Implementing the Council Regulation (EC) No 2252/2004 of 13 December 2004 on Standards for Security Features and Biometrics in Passports and Travel Documents Issued by Member States* (No 1710/05/EN-rev, WP 112, 2005).
6. ——, *Opinion 3/2012 on Developments in Biometric Technologies* (No 00720/12/EN, WP193, 2012).
7. ——, *Opinion 4/2007 on the Concept of Personal Data* (No 01248/07/EN, WP136, 2007).
8. ——, *Opinion 5/2010 on the Industry Proposal for a Privacy and Data Protection Impact Assessment Framework for RFID Applications* (No 00066/10/EN, WP175, 2010).
9. ——, *Opinion 9/2011 on the Revised Industry Proposal for a Privacy and Data Protection Impact Assessment Framework for RFID Applications* (No 00327/11/EN, WP180, 2011).
10. ——, *Opinion N° 3/2007 on the Proposal for a Regulation of the European Parliament and of the Council Amending the Common Consular Instructions on Visas for Diplomatic Missions and Consular Posts in Relation to the Introduction of Biometrics, Including Provisions on the Organisation of the Reception and Processing of Visa Applications (COM(2006)269 final)* (WP134, 2007).
11. ——, *Opinion No 7/2004 on the Inclusion of Biometric Elements in Residence Permits and Visas Taking Account of the Establishment of the European Information System on Visas (VIS)* (No 11224/04/EN, WP 96, 2004).
12. ——, *Working Document on Data Protection Issues Related to RFID Technology* (No 10107/05/EN, WP 105, 2005).
13. ——, *Working Documents on Biometrics* (No 12168/02/EN, WP 80, 2003).
14. Commission of the European Communities, *Communication form the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Radio Frequency Identification (RFID) in Europe: steps towards a policy framework* (COM (2007) 96 final, 2007).
15. Council of Europe, 'Accession by the European Union to the European Convention on Human Rights: Answers to frequently asked questions' (*Council of Europe, ,* 2011) <http://www.coe.int/t/dghl/standardsetting/hrpolicy/CDDH-UE/CDDH-UE_documents/EU_accession-QA_2011_en.pdf> accessed 14 May 2012.

16. ——, ‘Chart of Signatures and Ratifications (Convention for the protection of Human Rights and Dignity of the Human Being with regard to the Application of Biology and Medicine: Convention on Human Rights and Biomedicine CETS No.: 164)’ (*Council of Europe,*, 2012) <http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=164&CL=ENG> accessed 5 May 2012.
17. ——, ‘List of declarations made with respect to treaty No. 164’ (*Council of Europe,*, 2012) <http://conventions.coe.int/Treaty/Commun/ListeDeclarations.asp?NT=164&CM=&DF=&CL=ENG&VL=1> accessed 15 May 2012.
18. ePractice.eu, ‘eGovernment Factsheet - Germany - Legal framework’ (2010) <http://www.epractice.eu/en/document/288243> accessed May 25 2010.
19. European Commission D-GJ, Freedom and Security,, ‘Comparative Study on Different Approaches to New Privacy Challenges, in Particular in the Light of Technological Developments’ (2010) <http://ec.europa.eu/justice/policies/privacy/docs/studies/new_privacy_challenges/final_report_en.pdf> accessed 30 Janurary 2012.
20. European Commission, ‘Commission Proposes A Comprehensive Reform of the Data Protection Rules’ (2012) <http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm> accessed 30 Janurary 2012.
21. ——, ‘How Will the EU's Reform Adapt Data Protection Rules to New Technological Developments?’ (2012) <http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/8_en.pdf> accessed 30 Janurary 2012.
22. ——, ‘Proposal for A Directive of the European Parliament and of the Council on the Protection of Individuals with regard to the Processing of Personal Data by Competent Authorities for the Purposes of Prevention, Investigation, Detection or Prosecution of Criminal Offences or the Execution of Criminal Penalties, and the Free Movement of Such Data, (COM(2012) 10 final)’ (2012) <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0010:FIN:EN:PDF> accessed 30 Janurary 2012.
23. ——, ‘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)’ (2012) <http://ec.europa.eu/justice/data-

protection/document/review2012/com_2012_11_en.pdf> accessed 30 Janurary 2012.

24. ——, ‘Why Do We Need an EU Data Protection Reform?’ (2012) <http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/1_en.pdf> accessed 30 Janurary 2012.
25. European Parliament, Resolution of 5 May 2010 on the launch of negotiations for Passenger Name Record (PNR) agreements with the United States, Australia and Canada.
26. Foundation for Information Policy Research, *Paper No. 4: The Legal Framework: an Analysis of the "Constitutional" European Approach to Issues of Data Protection and Law Enforcement* (UK Information Commissioner Study Project: Privacy & Law Enforcement, 2004).
27. ——, *Paper No. 5: Conclusions & Policy Implications* (UK Information Commissioner Study Project: Privacy & Law Enforcement, 2004).
28. Information Commissioner Office, ‘The ‘Durant’ Case and Its Impact on the Interpretation of the Data Protection Act 1998’ <http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/the_durant_case_and_its_impact_on_the_interpretation_of_the_data_protection_act.pdf> accessed 9 June 2011.
29. International Organization for Standardization, ‘ISO 22307:2008: Financial services -- Privacy impact assessment, 16 Apr 2008.’ (2008) <http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=40897> accessed 20 Februrary 2012.
30. Laurie G and Sethi N, ‘Information Governance of Use of Patient Data in Medical Research in Scotland: Current and Future Scenarios’ (*Scottish Health Informatics Programme (SHIP)*) <http://www.scot-ship.ac.uk/sites/default/files/Reports/Scoping_Report_Final_August_2010.pdf> accessed 6 August 2011.
31. Privacy International, ‘PHR2006 - Republic of China (Taiwan) ’ (*Privacy International*, , 2007) <https://www.privacyinternational.org/category/countries/taiwan> accessed 5 March.
32. Reding V, ‘Towards A True Single Market of Data Protection (SPEECH/10/386, Meeting of the Article 29 Working Party, Review of the Data protection Legal Framework)’ (*The EU*, 2010) <http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/10/386>

accessed 24 April 2012.

33. Robinson N and others, *Review of the European Data Protection Directive* (Technical Report, 2009).
34. Scottish Health Informatics Programme (SHIP), 'SHIP Guiding Principles and Best Practices: A document of the SHIP Information Governance Working Group' (*Scottish Health Informatics Programme (SHIP)*, 22 October 2010) <http://www.scot-ship.ac.uk/sites/default/files/Reports/Guiding_Principles_and_Best_Practices_221010.pdf> accessed 17 October 2011.
35. The Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, 'Progress Report on the Application of the Principles of Convention 108 to the Collection and Processing of Biometric Data' (*T-PD*, 2005) <http://www.coe.int/t/e/legal_affairs/legal_co-operation/data_protection/documents/reports_and_studies_of_data_protection_committees/2Biometrics_2005_en.pdf> accessed 13 February 2010.
36. The European Data Protection Supervisor, 'Opinion of the European Data Protection Supervisor on a research project funded by the European Union under the Seventh Framework Programme (FP7) for Research and Technology Development - Turbine (TrUsted Revocable Biometric IdeNtitiEs)' (2011) <http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2011/11-02-01_FP7_EN.pdf> accessed 23 May 2012.
37. The European Data Protection Supervisor, '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, OJ 2008/C 101/01, 2007).
38. Zagoria DS, *The Taiwan Challenge* (the National Committee on American Foreign Policy presneted to the Asia Society, 2004).

Thesis

1. Alexander PM, 'Towards reconstructing meaning when text is communicated electronically' (PhD thesis, University of Pretoria 2002).

Web Pages

1. European Commission, '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)' (2012) <http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf> accessed 30 Janurary 2012.
2. NFC Forum, 'About NFC' (*NFC Forum*, 2012) <http://www.nfc-forum.org/aboutnfc/> accessed 10 July 2012.
3. Parliamentary Office of Science and Technology, 'Radio Frequency Identification (RFID)' (*Parliamentary Office of Science and Technology*, 2004) <http://www.parliament.uk/documents/upload/POSTpn225.pdf> accessed 18 November 2009.
4. The Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, 'Progress Report on the Application of the Principles of Convention 108 to the Collection and Processing of Biometric Data' (*T-PD*, 2005) <http://www.coe.int/t/e/legal_affairs/legal_co-operation/data_protection/documents/reports_and_studies_of_data_protection_committees/2Biometrics_2005_en.pdf> accessed 13 February 2010.

Others

1. Jain AK and Pankanti S, Beyond Fingerprinting: Is Biometrics the Best Bet for Fighting Identity Theft? (Scientific America Magazine 2008).
2. Klüver L, Peissl W and Tennøe T, *ICT and Privacy in Europe: Experiences from Technology Assessment of ICT and Privacy in Seven Different European Countries* (EPTA 2006).
3. Koorn R and others, *Privacy Enhancing Technologies –White Paper for Decision-Makers* (2004).
4. Robb D, *Authentication with a Personal Touch: Fingerprint Scanners Are Accurate Biometric Identification Tools - But They're Not Foolproof* (Government Computer

News, 2005 WLNR 26140142, 2005).