CONSUMER PROTECTION IN AN ELECTRONIC ENVIRONMENT

by

IYEN JOY AKHIGBE

Submitted in accordance with the requirements
for the degree of

DOCTOR OF LAWS
at the

UNIVERSITY OF SOUTH AFRICA

PROMOTER: PROFESSOR TANA PISTORIUS

DECEMBER 2020

DECLARATION

Name: Iyen, Joy Akhigbe
Student Number: 44684533
Degree: LL D

I declare that CONSUMER PROTECTION IN AN ELECTRONIC ENVIRONMENT is my own work and that all the sources that I have used or quoted have been indicated and acknowledged by means of complete references.

I further declare that I have not previously submitted this work, or part of it, for examination at UNISA or at any other higher education institution for any other qualification.

_____ _____

Signature **Date**

ACKNOWLEDGMENTS

I wish to thank my supervisor, Prof Tana Pistorius the incumbent of the South Africa Research Chair in Law Society and Technology (SARCHI), for her invaluable intellectual resources and guidance. Special thanks to the National Research Foundation and the UNISA community for awarding me a bursary towards the completion of my studies. I remember my first real contact with UNISA, Prof Anneliese Roos, and I am grateful to her for her immense contribution towards my success at UNISA. I acknowledge with thanks the support received from Dr Sheila Mavis Nyatlo, Prof Neville Botha, Karen Breckon of the UNISA library, Dr C Joelle Nwabueze Post-Doctoral Research Fellow SARCHI, UNISA, and the indefatigable Secretary to the SARCHI, College of Law, UNISA, Catherina Zaayman. My gratitude also goes to Prof Calboli Irene of the University of Texas A&M and Prof Rosen Jan of Stockholm University for their contributions.

Profound thanks goes to my husband Sir Dr EE Akhigbe, and my children whose time was consumed while working on my thesis. My mum, Lady Edith Edosa, my siblings Gloria and Emmanuel and their spouses, Paul and Eki, and of course, my guardian, Rev Fr Dr Peter A Egbe, are greatly appreciated for their unstinting support and encouragement. Special thanks to my mother-in-law, Dame E Akhigbe, and my sisters-in-law, Dame (Mrs) Mabel Izzi, Dr (Mrs) Stemillia Ewemade, and Dr (Mrs) Omoye West for their care. I remember with thanks the understanding and support received from my colleagues in the office who struggled with my time but with little success.

Finally, I thank my most respected friends and elders who kept on encouraging me, Sir Dr Rufus and Lady Lenette Ikharevbore, Prof NA Inegbedion, Prof SE Orobator, Rv Sr Esther Edeko (OLA), Hon Eunice Otoghile, and, of course, Weyimi R Wonodi.

Thank you all.

DEDICATION

To GOD Almighty

and

my dearest Daddy, Hon (Sir) SO Edosa, who passed on 14 April 2018.

ABSTRACT

Consumer protection laws have not evolved on par with the development of electronic media. As a result, consumer protection laws do not address all major areas of legal concern that affect the electronic commerce (e-commerce) consumer. Furthermore, differing laws in the area of consumer protection make harmonised consumer protection neigh on impossible.

Currently, there is a plethora of laws on the protection of consumers but most of these laws are within the sphere of conventional consumer protection legislation which does not adequately address the legal challenges posed by the proliferation of electronic transactions (e-transactions). Specific e-transaction laws are now to be found in certain international and regional documents emanating from organisations including: the United Nations (UN); the Council of Europe; the Organisation for Economic Cooperation and Development (OECD); the African Union (AU); the Economic Community of West African States (ECOWAS); the Southern African Development Community (SADC); the Common Market for Eastern and Southern Africa (COMESA); and the East African Community (ECA). These legal instruments have already been implemented in certain states' national legislation, while other countries have yet to accede to them. Despite these legal instruments, e-commerce consumers are faced with inadequate or obsolete legislative provisions and are yet to enjoy full protection equivalent to that accorded to the "traditional" consumer. Furthermore, given the trans-national nature of the internet, divergent laws will inevitably prove to provide inadequate protection to e-commerce consumers.

In this research, international and regional legislative instruments, as well as the national laws of selected countries such as the United States (US), the United Kingdom (UK), the Republic of South Africa (South Africa), the Federal Republic of Nigeria (Nigeria), and the Commonwealth of Australia (Australia) are examined. The strengths and gaps in each of these instruments and laws are identified with the aim of

harmonising the principles they espouse in a single, cogent, and comprehensive body of rules which could take the form of an international convention. An international convention should be based on national and international best practices. The national adoption of the minimum standards espoused in the proposed Convention will ultimately, promote harmonisation.

KEY WORDS

Borderless jurisdiction; cooling-off; cyberspace; e-agent; e-commerce consumer rights; electronic transferable record; hidden charges; information; keystroke error; m-commerce; online; shrink-wrap; single window facility; terms and conditions; transaction; web-wrap; wireless application protocol (WAP).

TABLE OF CONTENTS

LIST OF ABBREVIATIONS

3D	Three Dimensional
3G	Third Generation
4G	Fourth Generation
AAA	ASP Application Aggregator
AANOIP	African Academic Network on internet Policy
ACCC	Australian Competition and Consumer Commission
ACL	Australian Consumer Law
ADMA	Australian Direct Marketing Association
ADR	Alternative Dispute Resolution
AMS	Automated Message System
APC	Africa, Caribbean and Pacific Group of States
ARB	Advertising Regulatory Board
ARIN	American Registry for Internet Numbers
ARPA	Advanced Research Projects Agency
ARPANET	Advanced Research Projects Agency Network
ASA	Advertising Standards Authority
ASP	Application Service Provider
ATM	Automated Teller Machine
AU	African Union
Australia	Commonwealth of Australia
B2A/G	Business-to-Administration/Government
B2B	Business –to-Business
B2C	Business-to-Consumer
BBN	Bolt, Beranek and Newman
BBS	Bulletin Board Service
BSP	Business Service Provider
C2C	Consumer- to-Consumer
CAFCOM	Consumer Affairs Committee

CAN-SPAM Act	Controlling the Assault of Non-Solicited Pornography and Marketing Act
CAO	Consumer Awareness Organisation
CBN	Central Bank of Nigeria
CCA	Competition and Consumer Act
CCR	Consumer Contracts Regulation
CCP	Committee on Consumer Policy
CCTLD	Country Code Top Level Domain
CDA	Communications Decency Act
CDMA	Code-Division Multiple Access
CD ROM	Compact Disk Read-Only Memory
CID	Civil Investigative Demand
CISG	Contracts for the International Sale of Goods
CJEU	Court of Justice of the European Union
CLP	Computer Law Practice
CMA	Competition and Marketing Authority
COMESA	Common Market for Eastern and Southern Africa
CPA	Consumer Protection Act 68 of 2008
CPC	Consumer Protection Centre
CPCA	Consumer Protection Council Act
CPC Regulation	Regulation on Consumer Protection Cooperation
CPD	Consumer Protection Directive
CPP Act	Cybercrime Prohibition Prevention Act
CPR	(OECD) 2016 Consumer Protection in E-commerce: OECD Recommendation
CPRs	Consumer Protection from Unfair Trading Regulations
CRD	Consumer Rights Directive
CRM	Customer Relations Management
CSP	Content Service Provider
DARPA	Defence Advanced Research Projects Agency
DC	District of Columbia

DMASA	Direct Marketing Association of South Africa
DNS	Domain Name System
DDoS	Distributed Denial of Service
DoS	Denial of Service
DVD	Digital Versatile Disk
E-Agent	Electronic Agent
EAC	East African Community
E-business	Electronic Business
E-commerce	Electronic Commerce
E-commerce Regulation	Electronic Commerce Regulation
E-communications	Electronic Communications
EC Convention	United Nations Convention on the use of Electronic Communications in International Contracts
ECC	European Consumer Centre
ECCAS	Economic Community of Central African States
ECOWAS	Economic Community of West African States
ECTA	Electronic Communications and Transactions Act
E-documents	Electronic Documents
EDI	Electronic Data Interchange
EEC	European Economic Community
EFCJ Act	Enforcement of Foreign Civil Judgements Act
EFT	Electronic Fund Transfer
E-goods	Electronic Goods
E-intermediaries	Electronic Intermediaries
E-legislation	Electronic Legislation
E-mail	Electronic Mail
E-money	Electronic Money
E-service	Electronic Service
E-signature	Electronic Signature

E-Sign Act	Electronic Signatures in Global and National Conference Act
ESC	Economic and Social Council
ESN	Electronic Serial Number
E-tailing	Electronic Retailing
E-trade	Electronic Trade
ETA	Electronic Transactions Act
E-transactions	Electronic Transactions
E-transferable	Electronic Transferable
E-transactions Bill	Electronic Transactions Bill
EU	European Union
EULA	End User Licence Agreement
E-web	Electronic Web
FCA	Financial Conduct Authority
FCCPA	Federal Competition and Consumer Protection Act 2019
FOB	Free on Board
FRN	Federal Republic of Nigeria
FSP	Full-Service Provider
FTC	Federal Trade Commission
G2B	Government-to-Businesses
G2C	Government-to-Consumers
GA	General Assembly
GLO	Globacom Limited
GPS	Global Positioning System
HiFi	High Fidelity
HIPSSA	Harmonisation of ICT Policies in Sub-Saharan Africa
HTML	Hypertext Markup Language
ICASA	Independent Communications Authority of South Africa
ICC	International Chamber of Commerce
ICCPR	International Covenant on Civil and Political Rights
ICJ	International Court of Justice
ICT	Information Communications Technology

ICTL	Information and Communications Technology Law
IGAD	Intergovernmental Authority on Development
IIA	Internet Industry Association
IJRC	International Justice Resource Centre
IMEI	International Mobile Equipment Identity
INEC	Independent National Electoral Commission
IP	Internet Protocol
IR	Infrared Radiation
ISP	Internet Service Provider
ISV	Independent Software Vendor
IT	Information Technology
ITU	International Telecommunications Union
LAN	Local Area Network
LFN	Laws of the Federation of Nigeria
MAN	Metropolitan Area Network
Mbps	Megabits per second
M-commerce	Mobile commerce
M-consumer	Mobile consumer
MDAs	Ministries, Departments and Agencies
ML	Model Law
MLER	Model Law on Electronic Transferable Records
MMS	Multimedia Messaging Service
MS-DOS	Microsoft Disk Operating Systems
MSSSP	Managed Security Software Provider
MTN	Mobile Telephone Network
NAP	Network Access Point
NCA	Nigerian Communications Act
NCC	Nigerian Communications Commission
NCC	National Consumer Commission

NCOP	National Council of Provinces
Nigeria	Federal Republic of Nigeria
NIS	Nigerian Industrial Standard
NITDA	National Information Technology Development Agency
NORPRO	Norwegian Committee on Trade Procedures
NSF	National Science Foundation
NSFNET	National Science Foundation Network
NSP	Network Service Provider
OAU	Organisation of African Unity
ODR	Online Dispute Resolution
OECD	Organisation for Economic Cooperation and Development
OFT	Office of Fair Trading
OHADA	Organisation for the Harmonisation of Corporate Law in Africa
OSP	Online Service Provider
PC	Personal Computer
PCS	Personal Communications Services
PDA	Personal Digital Assistant
PDF	Portable Document Format
PoP	Point of Presence
POS	Point of Sale
PTA	Preferential Trade Area
PSP	Payment Services Provider
PSR	Payment Services Regulation
REC	Regional Economic Communities
RTV	Return to Vendor
South Africa	Republic of South Africa
SADC	Southern African Development Community
SADCC	Southern African Development Coordinating Conference
SATRA	South Africa Telecommunications Regulatory Authority
SC	Security Council
SGL	Sale of Goods Law

SI	System Integrator
SIM	Subscriber Identification Module
SLD	Secondary Level Domain
SMS	Short Message System
SON	Standards Organisation of Nigeria
SONCAP	Standards Organisation of Nigeria Conformity Assessment Programme
TI	Transmission System 1
TPS	Telephone Preference Service
TV	Television
UCITA	Uniform Computer Information Transactions Act
UDHR	Universal Declaration of Human Rights
UETA	Uniform Electronic Transactions Act
UK	United Kingdom
ULC	Uniform Law Commission
UN	United Nations
UN Charter	United Nations Charter
UNCITRAL	United Nations Committee on International Trade and Law
UNCITRAL Model Law	UNCITRAL Model Law on Electronic Commerce
UNCP	United Nations Guidelines for Consumer Protection
UNCTAD	United Nations Conference on Trade and Development
URL	Uniform Resource Locator
US	United States of America
USB	Universal Serial Bus
USC	United States Congress
USSR	Union of Soviet Socialist Republics
VANS	Value-added Network Services
VAR	Value Added Reseller
VCR	Videocassette Recorder

VPN	Virtual Private Network
WAEMU	West African Economic and Monetary Union
WAN	Wide Area Network
WAP	Wireless Application Protocol
WASPA	Wireless Application Service Provider Association
WD	Web Developer
Wi-Fi	Wireless Networking Technology of the Electrical and Electronics Engineers 802.11 Standards
WTO	World Trade Organisation
WWW	World Wide Web
XML	Extensible Markup Language

ABBREVIATION OF JOURNAL TITLES

AUJT	*Assumption University Journal of Technology*
BFLR	*Banking & Finance Law Review*
BLJ	*Banking Law Journal*
Brit YB Int L	*British Yearbook of International Law*
CBLJ	*Canadian Business Law Journal*
CILSA	*Comparative & International Law Journal of South Africa*
CLR	*Columbia Law Review*
CLSR	*Computer Law and Security Report*
EDI LR	*Electronic Data Interchange Law Review*
FIPMEL	*Fordham Intellectual Property Media & Entertainment Law*
ICCLR	*International Company and Commercial Law Review*
IJEC	*International Journal of Electronic Commerce*
JAMS	*Journal of the Academy of Marketing Science*
JIA	*Journal of International Arbitration*
JILT	*Journal of Information, Law and Technology*
JIPITEC	*Journal of Intellectual Property, Information Technology and E-Commerce*
JWT	*Journal of World Trade*
LJ	*Law Journal*
OJL	*Official Journal of the European Union Legislation*
PERJ	*Potchefstroom Electronic Law Journal*
RCTLJ	*Rutgers Computer and Technology Law Journal*
Rich JL & Tech	*Richmond Journal of Law & Technology*
SALJ	*South African Law Journal*
SA Merc LJ	*South African Mercantile Law Journal*
SRJIS	*Scholarly Research Journal for Interdisciplinary Studies*
Stell LR	*Stellenbosch Law Review*
THRHR	*Tydskrif vir Heedendaagse Romeins-Hollandse Reg*

WLR *Washington Law Review*

LIST OF DIAGRAMS & TABLES

DIAGRAMS

TABLES

CHAPTER ONE

EXPOSITION OF THE STUDY

1.1 Introduction: The concept of consumer protection

With the advent of computers and their ability to connect to millions of other computers across the globe in seconds through networks, a new legal challenge has emerged in the protection of consumers of electronic goods (e-goods) and services.

Electronic commerce (e-commerce) consumers cut across users of all forms of electronic technologies, communications and media: wearables; services such as third generation (3G) and fourth generation (4G) technology; cell phones; landlines; broadband; wireless networking technology of the Electrical and Electronics Engineers 802.11 standards (Wi-Fi);[1] satellite; home dial-ups; and, of course, the computer. These communication media are used for internet telephony, the sending of electronic mails (e-mails), online shopping, contract conclusion, news transmission, file-sharing/data transfer, online gambling, streaming, multiplayer gaming, money transfer, electronic payments (e-payments), and other forms of commercial transactions. In recent years, most forms of trade or commercial activity have been initiated, managed, and concluded online.

Before the influence of information technology (IT) on electronic applications, consumer protection was promoted through consumerism.[2] Cranston[3] defines consumerism as the "actions of individuals and organisations in response to consumer

---

1 Wi-Fi is a wireless network that works with a technology through which devices communicate without the use of internet cords, available at https://www.lifewire.com (date of use: 07 February 2020).

2 Consumerism is used in reference to consumer protection, or consumer activism, which seek to protect and inform consumers on their rights as well as require that producers and manufacturers deal fairly with consumers see Ogechukwu (2013) 5/1 *International Postgraduate Business Journal* 2 & 5.

3 Cranston *Consumers and the Law* 1.

dissatisfaction arising in exchange relationships".[4] He further notes that "consumerism is a protest against perceived business injustices and efforts to remedy them".[5] In the *Oxford English Dictionary*,[6] consumerism is defined simply as protection of the consumer's interest.

According to Prosser,[7] early legislative action on consumer protection dates back to 1266 English legislation imposing criminal liability on supplies of corrupted food. The United States of America (US) also saw attempts at consumer protection as early as 1890 under the Sherman Antitrust Act. By the 1970s there were widespread consumer protection laws across various jurisdictions.[8]

Consumers were further protected under common law in common-law jurisdictions such as Nigeria and the United Kingdom (UK). Certain consumer protection offences, such as the sale of contaminated or expired goods,[9] were fully prosecuted under criminal law and consumers' rights were enforced through the laws of tort and contract. The principal challenge facing the protection of consumers before the evolution of computers, centered on choice of law and the determination of applicable jurisdiction where consumer transactions involved distance trade. To this end, the Rome Convention of 1980[10] established uniform rules concerning the law applicable to contractual obligations.

---

4 Ibid.

5 Ibid.

6 *Oxford English Dictionary* 210.

7 Prosser (1960) 69 *Yale LJ* 1099 at 1103 cited in Clark *Product Liability* at 2.

8 In South Africa, for instance, there was the Price Control Act 25 of 1964, the Trade Practices Act 76 of 1976, as well as some other Acts relating to consumer protection. These, and related Acts were repealed by the Consumer Protection Act 68 of 2008 (CPA); see also, the Australian Trade Practices Act, 1974, now replaced by the Competition and Consumer Act, 2010.

9 The offence was contained in the Food and Drugs Act, 1974, which was later repealed by the Food and Drugs Act Cap 150, Laws of the Federation of Nigeria, 1990.

10 The Rome Convention 80/934/EEC on the law applicable to contractual obligations was converted into a Community Regulation, Regulation (EC) 593/2008 of the European Parliament and of the Council of Europe of 17 June 2008 on the law applicable to contractual obligations (Rome 1 Regulation).

However, by the late 1970s online applications had been developed,[11] and by the 1980s other applications such as Electronic Fund Transfer (EFT) and Electronic Data Interchange (EDI) were in everyday use. In 1990, the World Wide Web (WWW) protocol was created by Berners-Lee, and by 1992 the first online bookstore was opened by Charles Stack.[12] This was followed by further technological innovations from 1994 to date such as online banking, e-mail contracting, and web-shopping. These developments led to the opening of an online pizza shop by Pizza Hut in 1994.[13] Immediately thereafter, Amazon.com opened its shopping site online in July 1995,[14] followed by eBay in September 1995.[15] Consumer response to e-commerce and mobile commerce (m-commerce) was overwhelmingly positive. Consumers were attracted by its high levels of convenience, wider selections, competitive pricing, and increased access to information.[16]

1.2 Research interest

The growth in internet usage has risen exponentially from less than one per cent in 1995, to approximately 58.8 per cent in 2019.[17] As of 30 June 2019, internet users worldwide stood at some 4,536, 248,808.[18] Based on a 2018 study, internet users who researched products or services online before actually making major purchases were in the region of 82 per cent.[19] As of 2018, the rate of online retail shopping was

11 Micheal Aldrich invented online shopping in 1979, see Aldrich "Internet online shopping" available at www.aldricharchive.com/internet_shopping.html (date of use: 12 July 2020).
12 Ibid.
13 Pizza Hut "Pizza Hut celebrates 20th anniversary of world's first online purchase with 50 per cent off online deal for Hut lovers members" available at https://prnewswire.com (date of use: 02 September 2020).
14 Rushton "The History of Amazon.com" available at https://www.techwalla.com (date of use: 03 August 2020).
15 Waxman "eBay 20th Anniversary: First Item Sold" available at www.time.com (date of use: 02 October 2020).
16 Jarvenpaa & Todd (1997) *IJEC* 59; see also Peterson, Balasubramanian and Bronnenberg (1997) *JAMS* 329-330.
17 Internet Usage and World Population Statistics estimates for June 30, 2019 sourced from Internetworld Stats "Internet world statistics" available at www.internetworldstats.com (date of use: 27 November 2020).
18 Ibid.
19 Ellet "New research shows growing impact on online research on in-store purchases" available at https://www.forbes.com (date of use: 03 October 2020).

measured at approximately 8.8 per cent globally.[20] This lends credence to the claim that "e-commerce is no longer a prediction but an economically significant reality."[21] From the foregoing, it is only to be expected that the increase in e-commerce (which includes the use of smartphones, wearables, tablets, etc. – hereafter collectively referred to as m-commerce) will continue to escalate. Clearly, we are living in the "mobile age;" an age in which m-commerce has been firmly established.[22]

The paradigm shift from the conventional methods of commerce and paper-based contracting to e-commerce generates new challenges with regard to the provision of electronic equivalents to writing and signature. These challenges require legal responses, among which is the legal recognition of electronic messages (e-messages) in order to secure their evidential value and legal validity. To date, however, responses have been coordinated differently at regional and national levels through the enactment of various e-commerce laws. However, the different rules contained in these national laws create disparate and fragmented regulations and this has a negative impact on consumers who trade across borders. For instance, a European who purchases software from a South African web store may not be informed of issues with interoperability of the software. The consumer will, therefore, be unable to seek redress as the applicable South African law on e-commerce has no requirement for the provision of information on interoperability of software. The legal challenges presented with e-commerce include the effect of consumers being subject to different national laws in respect of their online transactions while at the same time having less protection than conventional consumers.

In recognition of the global nature of the internet it has, therefore, become necessary to provide for a comprehensive and internationally-accepted set of principles that will

20 Saleh "Global online retail spending – statistics and trends" available at www.invespcro.com (date of use: 03 October 2020).
21 Snail *15 Juta Business Law* (2007) 41; see also Kidd and Daughtery (2000) 26 *RCTLJ* 232.
22 Rowland, Kohl and Charlesworth *Information Technology Law* 233.

serve as minimum standards in respect of all e-commerce consumer transactions in order to create uniformity and certainty.[23]

To achieve the primary focus of this research, it is necessary to limit the parameters of the study to legislation, cases, and materials which touch directly on the protection of consumers who transact by electronic means. The study will, therefore, not undertake a contextual analysis or examination of legislation, cases, or materials dealing with general aspects of consumer protection; nor will it consider the principles of consumer protection through contract, delict, or tort, save by way of reference.

1.3 Problem statement

In providing for e-commerce consumer protection rules, a variety of constraints arise as the internet is faceless and without borders. The research problems could, therefore, be summarised as tripartite in nature.

1. The existing regulatory framework for the protection of e-commerce consumers in international, regional, and selected jurisdictions is limited in scope. Recondite issues such as the rights of e-commerce consumers, jurisdiction, implementation, and enforcement of foreign judgments are not exhaustively addressed.
2. Most consumer-protection rules applicable to e-commerce consumers are out-dated as they do not address all issues arising in the marketplace. There are no proper standards in some jurisdictions in respect of emerging issues arising from technological advances such as single-window facilities; automatically generated electronic transferable (e-transferable) records; interoperability; online auctions; advances in artificial intelligence act and data processing by electronic agents (e-agents). This exacerbates fragmentation and the erosion of gains achieved in terms of legal certainty.

[23] A case for legal certainty in electronic contracts (e-contracts) is made by Eiselen in “Purpose, Scope and underlying principles of the UNECIC” 106.

3. Some countries have no legislation to protect e-commerce consumers due to the lack of political will of the leaders of those countries to assent to and domesticate regional and international rules on e-commerce.

1.3.1 The role of law in the determination of legal certainty in e-commerce

One characteristic of law is that it is dynamic and must follow change. Pound once wrote that "the law must be stable, yet it cannot stand still."[24] The German lawyer and sociologist, Max Weber,[25] postulates that law should be rational. Rationality, in his view, presents two aspects: one, a formal logical aspect based on intellectual consistency between legal rules, principles, standards, and concepts; and the other, a substantive ideological or value aspect in the sense of conformity with the changing values of society.[26] The first is relatively static, the second dynamic.[27] Society has moved with the development of information communication technology (ICT) and has embraced e-commerce, but the law has been left behind. Paragraph 2 of the Preamble to the Southern African Development Community (SADC) Model Law on Electronic Transactions and Electronic Commerce,[28] aptly captures the position of the law as it existed before the adoption of e-commerce-specific laws, as follows:

> The principles of contract law are old: they were formed in a paper-based world that ran on paper and ink. The meeting of minds in cyberspace was never envisaged, and the validity and effect of using electronic messages in commercial communications were never contemplated. Requirements such as writing and signature cannot be translated to the virtual and paperless world of e-commerce without legislative intervention.

While electronic trade (e-trade) was fostered without a regulatory framework, specific legal responses to legal aspects related to e-commerce and consumer protection began to emerge from regional and international bodies in the late 1980s.[29] These

---

24 Pound *Interpretations of Legal History* 13.
25 Weber *Law in Economy and Society* 6.
26 Ibid.
27 Farrar and Dugdale *Legal Method* 11.
28 Southern African Development Community (SADC) Model Law on Electronic Transactions and Electronic Commerce, 2012.
29 See for instance the recommendation contained in Official Records of the General Assembly,

legal responses related to various issues including the legal validity of e-communications, electronic signatures (e-signatures), secure payment systems, unsolicited goods and spam, and consumer rights. The drive for regulation by international organisations[30] was based on the need for harmonisation as these technological trends had broken through geographic barriers and made the world one location, one market, which, therefore, demanded one law. These regulations were drafted by bodies such as the United Nations (UN);[31] the European Union (EU);[32] the Organisation for Economic Co-operation and Development (OECD);[33] and, very recently, the African Union (AU).[34] In addition, there are Model Laws from the Common Market for Eastern and Southern Africa (COMESA);[35] the Southern African Development Community (SADC);[36] the Economic Community of West African States (ECOWAS);[37] the East Africa Community (EAC);[38] and the Organisation for the Harmonisation of Business Law in Africa (OHADA).[39] There is also a draft Model Law on Electronic Transactions (e-transactions) from the Commonwealth.[40]

Fortieth Session, Supplement No 17 (A/40/17) chap vi section B on the legal value of computer records, this recommendation was adopted by the Commission at its eighteenth session in 1985.

30 See paras 1 and 2 of the Preamble to the UNCITRAL Model Law on Electronic Commerce 1996 (UNCITRAL Model Law); see also Preamble to Directive 2000/31/EC of the European Parliament and of the council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the internal market OJ L 178, 17/07/2000 P.0001 -0016 (E-commerce Directive) particularly paras 5 and 7.

31 UNCITRAL Model Law; United Nations Convention on the use of Electronic Communications in International Contracts (EC Convention) (Res 60/21 2005).

32 Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on Certain Legal Aspects of Information Society Services in Particular Electronic Commerce in the Internal Market (E-commerce Directive); Directive 2011/83/EC of the European Parliament and of the Council of 25 October 2011 on Consumer Rights (CRD).

33 OECD (2016) Consumer Protection in E-Commerce: OECD Recommendations (CPR); Guide lines for Protecting Consumers from Fraudulent and Deceptive Commercial Practices across Borders (Consumer Protection Guidelines) 2003.

34 African Union Convention on the Establishment of a Legal Framework Conducive to Cyber Security in Africa (AU Convention) 2014.

35 Model Law on Electronic Commerce (COMESA Model Law) 2010.

36 Southern African Development Community (SADC) Model Law on Electronic Transactions and Electronic Commerce (SADC Model Law) 2012.

37 Supplementary Act A/SA.2/01/10 on Electronic Transactions in the ECOWAS Area adopted at the 37th Session of the Authority of Heads of State and Government, Abuja 16 February 2010.

38 EAC Framework for Cyberlaws Phase I 2008 and Draft EAC Framework II 2011.

39 Uniform Act Relating to General Commercial Law 2014 (Uniform Act).

40 The Draft Model Law on Electronic Transactions was drafted on the basis of the outcome of the

The efforts of these international and regional bodies elicited responses from over 49 countries so that from about 1998 to date, these countries have been influenced to enact national laws to provide protection for the e-commerce consumer.[41] These laws notwithstanding, it will emerge in the course of this research that the protection of an e-commerce consumer is not yet settled law as the regional and international instruments in force are not sufficiently comprehensive to provide adequate protection for the e-commerce consumer. This is exacerbated by the fact that certain countries

Commonwealth Law Ministers' meeting in July 2000 and recommendations for the Model Law were presented to the Commonwealth Senior Law Officials Meeting in 2001. A draft of the Model Law was circulated for consideration in 2002. The Commonwealth Model Law is largely identical to the UNCITRAL Model and consequently the provisions of the Commonwealth Model Law are not considered in this study. More information is available at www.thecommonwealth-ilibrary.org (date of use: 30 October 2020).

41 Examples of such countries and their laws include: Austria – Electronic Commerce Act, 2002; Azerbaijan Law on Electronic Trade, 2005; Bahamas – Electronic Communications and Transactions Act, 2003; Belgium – e-Commerce Laws, 2003; Belize – Electronic Transactions Act, 2003; Bermuda – Electronic Transactions Act, 1999; Brunei – Electronic Transactions Act, 2001; Canada – Electronic Communications Act, 2000; Colombia – Law 527/1999; Croatia – Electronic Communications Act, 2003; Czech Republic – Certain Information Society Services Act, 2004; Denmark – e-Commerce Act, 2002; Dominican Republic – Law 126/02 on Electronic Commerce, Digital Documents and Signatures, 2002; Ecuador – Law on Electronic Commerce, Electronic Signature and Electronic Data, 2002; Estonia – Information Society Services Act, 2004; Finland – Act on the provision of Information Society Services, 2002; Guatemala – Act for the Recognition of the Communications and Electronic Signatures, 2008; Iceland – Act on Electronic Commerce and other Electronic Services, 2002; Iran – Electronic Commerce Law of the Islamic Republic of Iran, 2004; Italy – Legislative Decree on Electronic Commerce, 2003; Jamaica – The Electronic Transactions Act, 2007; Jordan – Electronic Transactions Law, 2001; Kenya – Kenya Communications (Amendment) Act, 2009; Latvia – Information Society Services Act, 2004; Liechtenstein – Law on e-Commerce, 2003; Luxembourg – e-Commerce Act, 2000; Macedonia – Law on Electronic Commerce, 2007; Malaysia – Electronic Communications Act, 2006; Malta – Electronic Communications Act, 2002; Mauritius – Electronic Transactions Act, 2000; New Zealand – Electronic Transactions Act 2002; Norway – e-Commerce Act, 2003; Pakistan – Electronic Transactions Ordinance, 2002; Philippines – Electronic Communications Act, 2000; Poland – Act on Electronic Payment Instruments, 2002, and Act on Providing Services by Electronic Means, 2002; Samoa – Electronic Transactions Act, 2008; Saudi Arabia – Electronics Transactions Act, 2007; Singapore – Electronic Transaction Act, 1998; Slovenia – Electronic Communications and Electronic Signature Act, 2000; Spain – Law on Information Society Services and Electronic Communications, 2002; Sri-Lanka – Electronic Transactions Act, 2006; Tunisia – Law on Trade and Electronic Communications, 2000; United Kingdom – Electronics Commerce Regulations 2002; United States of America – Uniform Electronic Transactions Act, 1999; Vietnam – Decree on e-Commerce, 2006. These Acts are available at www.ictparliament.org/legislationlibrary/e-Commerce - archived (date of use: 12 April 2015). From additional sources there are the following laws: Cape Verde – Use of E-contracts, Signatures and Admissibility of Electronic Evidence in Courts, 2000; Republic of South Africa – Electronic Communications and Transactions Act, 2002; Australia – Competition and Consumer Act, 2010; Egypt – Law 15/2004 on E-Signature and Establishment of the Information Technology Industry Development Authority (ITIDA); and Morocco – Comite Interministeriel pour le Developpement et la Promotion du Commerce Electronique 2010, see Faria "Model laws as tools for legal harmonisation" 13.

are yet to assent to any of the international or regional documents on e-commerce or adopt any equivalent law.[42]

1.3.2 Research questions

The questions addressed in this research are:

(1) What problems face the e-commerce consumer?

(2) Using Nigeria as an example, to what extent can e-commerce consumers receive adequate protection from conventional consumer protection laws?

(3) Is subsisting e-commerce regulation able to address all the concerns raised by e-commerce transactions?

(4) Have divergent regulations in e-commerce contributed to the problem of inadequate protection for e-commerce consumers?

(5) What principles, measures, or rules need to be put in place to adequately protect e-commerce consumers?

1.3.3 Aims and objectives of the study

The principal aim of this study is to consider whether e-commerce consumers, in general, can be protected within the provisions of conventional legislation on consumer protection enacted before the inroads of e-commerce in countries where there are no specific e-commerce and e-commerce consumer-protection-related laws.[43] This research also examines international and regional conventions, model

---

42 It took Nigeria eight years before a Bill on E-transaction could pass the third reading at the House of Senate and that is the Electronic Transactions Bill 2017 and this Bill has not been accented to. Nigeria had two different Bills which were proposed for electronic transactions. The first was the Electronic Communication and Transactions Bill, 2009, followed by the Electronic Transactions (Establishment) Bill, 2013, which was subsequently amended as the "Electronic Transactions Bill, 2017". The Nigeria Cybercrimes (Prohibition, Prevention, etc) Act, 2015, also provides some measure of protection for e-commerce consumers. Countries like Sierra Leone and some others are yet to legislate on e-transactions, while some other countries have draft laws that are in legislative processes. In this regard see UNCTAD *Review of E-commerce Legislation harmonization in the Economic Community of West African States* available at http://unctad.org/PublicationsLibrary.pdf (date of use: 16 August 2020).

43 Seventy-nine per cent of countries of the world have legislation on e-transaction while fifty-two per cent have legislation on consumer protection. In Africa, fifty-four per cent of African countries have legislation on e-transaction, thirty-five per cent on consumer protection, twenty-two

laws and guidelines, as well as national legislation on e-transaction and consumer protection with a view to identifying gaps and grey areas requiring amendment. It further proposes a more comprehensive body of principles and measures which will serve as minimum requirements for the protection of the rights of consumers who transact online across the globe in the form of an international Convention or model law.

The research, therefore, is intended to achieve the following objectives:

1. To show the inadequacy of conventional consumer-protection legislation in protecting e-commerce consumers in general, but more specifically in countries with no specific e-commerce legislation, using Nigeria as an example.[44]
2. To carry out a comparative and in-depth study of relevant literature, legislation, model laws and guidelines on e-commerce with a view to identify areas requiring consumer protection.
3. To identify the challenges in implementing and enforcing national and international laws and regulations for the protection of e-commerce consumers.
4. To advance options for the proper implementation and functioning of consumer-redress systems, such as alternative dispute resolution (ADR) and online dispute resolution (ODR), and the recognition and enforcement of foreign judgments.
5. To propose an international framework for the protection of e-commerce consumers which embodies the basic elements of consumer-protection

per cent which includes Nigeria, Ethiopia; Guinea-Bissau amongst others have draft legislation while seven per cent do not have e-transaction or consumer protection laws (the countries without e-transaction or consumer protection laws include Angola; Chad and Gabon). Seventeen per cent of the countries in Africa do not have available data on the state of their laws on e-transaction and consumer protection; see UNCTAD "Summary of adoption of e-commerce legislation worldwide" available at www.unctad.org/en (date of use: 03 July 2020).

44 As earlier mentioned, although the Bill has passed the third reading, it is yet to receive Presidential assent. The E-transactions Bill is not listed among the Acts of the National Assembly, see https://nass.gov.ng (date of use: 20 June 2020). In the absence of a Presidential assent, the Constitution of the Federal Republic of Nigeria (1999) ss 58(1) & (5) empowers the National Assembly to override the veto powers of the President by passing the Bill again with a two-third majority. This process has not been followed.

measures especially in the electronic environment, and which will serve as minimum requirements for all jurisdictions.

1.3.4 Methodology

The protection of consumers who transact electronically is an emerging field of law as a result; African scholarly contributions and sources from case law are at present minimal. The purpose of this research is to add to the body of knowledge in this field, and to promote principles that will adequately protect the interest of consumers. To achieve this, the research adopts the following approaches.

(i) Comparative law approach

In order to establish basic elements of consumer protection for e-commerce consumers, relevant model laws from the United Nations and from Africa as well as the national laws of selected countries are analysed. The countries selected for this study are Nigeria and South Africa as African countries; the US for its highly advanced level of application of information technology (IT); and the UK as a prominent country that implemented EU legal instruments in her national laws.[45] The Commonwealth of Australia is also briefly considered with the expectation of providing insights into how this "other continent" approaches the research topic particularly with respect to implementation. Furthermore, no thorough interrogation of the topic would be complete without first considering international perspectives on what is, in essence, a global phenomenon. In this light, relevant documents from international and regional bodies such as the UN, the EU, the OECD, the AU, the ECOWAS, the SADC, the COMESA, the EAC, and the OHADA are examined.

---

45 Although on 23 June 2016 the UK voted to leave the EU, a single market of 28 countries in Europe, and the process got underway at the end of March 2017 when article 50 of the Treaty of Lisbon was invoked. This provision allows the UK and the EU to have two years to reach an agreement on splitting; until then the UK remains foremost in the implementation of EU Directives and Policies, see BBC News 29 March 2017 "Article 50: UK set to formally trigger Brexit process" available at www.bbc.com (date of use: 16 October 2020).

(ii) Private-law approach

A private-law approach is deemed helpful in that consumer protection law is regarded as an area of private law since it deals with private-law relationships between individuals or individuals and institutions.[46] In dealing with consumer protection on the internet, an international perspective on the private-law approach is adopted.[47] Drawing on the writings of Hay *et al*,[48] the theories of universalism and particularism[49] are used to develop international private-law rules. According to Hay and his co-authors, particularism focuses on the development of international private-law rules in tandem with the development of substantive law in the forum state.[50] Particularism also centers on reflecting national interests in international private-law rules.[51]

The universalist approach ensures that international private-law rules provide predictable results.[52] A universalist approach upholds international private law as "primarily a coordinating task for uniformity of result and decisional harmony."[53] Again, the universalist approach seeks to ensure that foreign judgments are given equal recognition and enforcement, and this limits "forum shopping."[54] The combination of the theories of both particularism and universalism compliment the objective of substantive law, namely to dispense justice in a cross-border dispute with a certain level of predictability. From the foregoing, particularism is a means of justifying universalism in cross-border consumer-protection principles under the private - law approach.

46 Smits *Advanced Introduction to Private Law* 1; see also Loos "The influence of European consumer law" 3.
47 Goldring (1996) 2/2 *Journal of Computer Mediated Communication* 4.
48 Hay, Lando and Rotunda "Conflict of Laws" 168.
49 Hay, Lando and Rotunda "Conflict of Laws" 172.
50 Hay, Lando and Rotunda "Conflict of Laws" 167-168.
51 Hay, Lando and Rotunda "Conflict of Laws" 172.
52 Vonken "Balancing Processes in International Family Law" 172.
53 Ibid.
54 Hay, Lando and Rotunda "Conflict of Laws" 167.

(iii) Legal positivist approach

Consumer protection is created by statute particularly more so for the protection of conventional consumers who trade outside the use of an electronic interface. However, current trends in law and commerce have necessitated the development of model laws by various regions and institutions and these laws are being incorporated into national legislation or ratified into use. The study, therefore, incorporates a positivist approach in which extant pieces of legislation are studied in detail in order to identify their areas of strength and weakness as regards consumer protection. This approach ensures that the essential elements of the law are identified and incorporated into proposals for new legislation in countries without protection for consumers in the context of e-commerce. The approach will at the same time inform recommendations for a framework which embodies the basic elements or principles adequate to protect e-commerce consumers, and which is suited to establish minimum requirements for the global community.

(iv) Theoretical use of primary and secondary sources

In a topic of so wide an application as consumer protection, great reliance is of necessity placed on primary sources such as the legal instruments and documents of international institutions. Legislation and case law from the Commonwealth of Australia, Nigeria, South Africa, the UK, and the US are consulted alongside secondary sources from the internet, books, and academic journals.

1.4 Chapter synopsis

One of the objectives of this study is to promote an effective state of law where consumers who transact online are not disadvantaged in comparison to conventional consumers. For this purpose, some international, regional, and national instruments were studied in Chapters Three to Six. In Chapter Four the comparison looks at the relevant EU Directives and the Australian ETA, reference to UK legislation is made as

they are a direct implementation of the EU Directives as observed in the chapter. For the African perspective the AU Convention, other regional instruments and the South African ECTA are the points of reference, while the UETA is used as the major instrument for analysing e-commerce consumer protection in the US.

The current chapter (Chapter One) offers an analytical look at the concept of e-commerce consumer protection. The interest in the research is identified, and the parameters of the study are set out. In this chapter, the role of law in shaping the future of e-commerce is summarised. E-commerce consumers need to have confidence in the electronic marketplace. Confidence can only be built through rules that adequately protect consumers in all aspects of their day-to-day transactions on the internet. These rules should embody minimum standards which can be implemented and enforced across all jurisdictions. There should be a system for redress, such as ADR or ODR; which is quick, user-friendly, accessible, and cost-effective. The various laws considered in this study are identified in this chapter and the path of study is mapped out in the methodology.

Chapter Two is an exposition of relevant terms and key concepts. The chapter delves into the historical background of the internet from a research network, to a global phenomenon. The terms considered include: “chargeback”, “computers”, “consumer”, “distance trade”, “e-commerce”, “e-agent”, “electronic intermediaries” (e-intermediaries), “internet”, “internet tools”, “key-stroke errors”, “shrink wraps”, and “web wraps”. The rights of consumers to review orders, correct mistakes, withdraw an order, cancel, refund, demand performance, reject unsolicited goods, and to have secured payment systems available, are all spelt out.

The protection of the rights of consumers transcends national boundaries by the very nature of the internet. Chapter Three, therefore, analyses the underlying principles of consumer protection from an international perspective, through the UN Convention on

the Use of Electronic Communications in International Contracts (EC Convention)[55] and the UNCITRAL Model Law on Electronic Commerce (UNCITRAL Model Law).[56]

In Chapter Four, the legal instruments of the EU and OECD on the protection of consumers who engage in e-commerce are examined. This study shows that most countries have implemented the legal acts at the regional level in their national laws. In Europe, for example, all EU member states have implemented the E-commerce Directive[57] in their national laws.[58] One can safely argue, therefore, that there is some measure of harmonised consumer protection within the EU. Although EU Community laws are transposed into national laws by member states, the level of protection appears inadequate in view of the fragmented nature of its implementation in some country's national laws. To drive home the unification objective of the EU community laws, the national laws of the United Kingdom will be examined with a view to ascertain the level of success in implementing EU Community laws in the area of e-commerce and the protection of e-commerce consumers. Closely linked to the EU geographically is the continent of Australia. The chapter, therefore, considers the applicable legal instruments on e-commerce in Australia and attempts to measure its level of protection for e-commerce consumers.

Chapter Five continues with the regional study of the underlying principles of consumer protection in the African continent. In the wake of the increased use of ICT in Africa, developing an African platform for consumer protection, akin to that of the

---

55 United Nations Convention on the Use of Electronic Communications in International Contracts Res 60/21 2005 adopted 23 November 2005 and entered into force 1 March 2013 (the Convention is enacted nationally in 11 Countries) available at www.uncitral.org (date of use: 11 October 2020).

56 General Assembly res 51/162 of 16 December 1996 adopted by the United Nations Commission on International Trade Law (UNCITRAL) Model Law on Electronic Commerce (with additional art 5*bis* adopted in 1998).

57 Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market *OJL* 178, 17.7.2000 1-16 (E-commerce Directive).

58 E-commerce Directive art 21-22 provides that member states should bring into force all that is necessary to comply with the transposition of the Directive before the 16 January 2002.The deadline for the transposition was 17 July 2003 see "Electronic Commerce Directive" available at www.eur-lex.europa.eu (date of use: 20 October 2020).

EU, and harnessing these opportunities together with other continents of the world, has become a pressing need. The establishment of an effective consumer protection regime in Africa is paramount. In this chapter, regional instruments which enable the protection of consumers in Africa are considered, a number of these instruments yet await state assent and domestication. The instruments originate from a wide range of African institutions representing West Africa, East Africa, Southern Africa, and other regions in Africa. These institutions include the AU, the ECOWAS, the COMESA, the SADC, the EAC, and the OHADA. Among African Countries, South African legislative framework for the protection of e-commerce consumers is most advanced. In this context, the protection of e-commerce consumers in South Africa is benchmarked against available protection as provided in regional documents in Africa.

A comparative-law approach necessitates an evaluation of other legal systems and the possible impact of transposing these principles into an existing legal system in order to strengthen it. The next chapter in this research, therefore, examines the level of protection for e-commerce consumers in the US through legislative provisions and case law. Chapter Six succinctly draws insights from the growth of e-commerce and the development of consumer-protection-related laws in the US. The principles on jurisdiction, choice of law, and the liability of intermediaries are well founded in case law and are unprecedented.

Chapter Seven is a review and analysis of all the comparative chapters. It sets out their areas of similarities and draws distinctions in their approach to the basic principles of e-commerce and consumer protection. The levels of implementation of the various laws are highlighted and this helps in drawing conclusions on the impact of these laws on consumers. From the comparative analysis an understanding of which countries have structures and agencies for the enforcement of the rights of e-commerce consumers is also possible.

In Chapter Eight, the position obtaining in Nigeria is examined. Existing rules governing consumer protection based on contracts are analysed and benchmarked

against current trends and laws on e-commerce. The efficacy and the protection of e-commerce consumers in the absence of e-commerce-specific legislation through the principles set out in substantive laws on consumer protection, unfair trade terms, jurisdiction, and choice of law is considered.

There has been different proposals for the adoption of legislation to protect consumers of e-goods and services, and the most recent is the Electronic Transactions Bill, 2017[59] Earlier in 2015, the CyberCrimes (Prohibition, Prevention, etc) Act,[60] was enacted containing several provisions on cybersecurity and the protection of computer systems and networks, e-communications, data, and computer programs, intellectual property, and privacy rights. The relevant provisions of the CyberCrimes (Prohibition, Prevention, etc) Act and those of the Electronic Transactions Bill (E-transactions Bill) are analysed.

Chapter Nine is a summary of the findings of and conclusions drawn from the evaluation of different international, regional, and national instruments dealing with e-commerce. In this chapter, a case is made for the need for an e-commerce specific legislation and for the harmonisation of e-commerce consumer-protection principles. E-commerce consumers engage with service providers globally. E-commerce consumers should enjoy the same basic and uniform level of protection wherever they may be domiciled. This also allows for predictability in the choice of law and enforcement of foreign judgments. The chapter introduces options which will grant respite for e-commerce consumers. One such option is recourse to accessible, affordable, and speedy means of seeking redress through ADR or ODR. In this chapter recommendations for more up-to-date principles are made. The chapter sets out salient elements for legislative consideration if an effective legal regime of protection for e-commerce consumers is to be actualised globally.

---

59 At the second session of the 8th National Assembly on 18 May 2017 “Votes and Proceedings”, a report of the Conference Committee on Electronic Transactions Bill, 2017, was presented in two versions (House of Representatives, and Senate) and the Senate version of the Bill was adopted, available at https://www.nassgov.ng (date of use: 20 June 2020). However, the Bill is not yet an Act in the absence of a Presidential assent, see footnote 44 above.

60 Cybercrime (Prohibition, Prevention, etc.) Act, 2015.

CHAPTER TWO

ELECTRONIC COMMERCE AND THE CONSUMER IN PERSPECTIVE

2.1 Introduction: The electronic environment

The development of the law of contract, delict, unfair business practices, and credit transfers revolved around conventional business practices until the emergence of IT in the commercial world. Under the conventional regime, parties have physical contact, are able to inspect goods or services physically, they bargain, and operate within defined geographic locations. The proximity and defined status of parties notwithstanding, legal issues in commerce are replete with uncertainties, especially in international trade.[1] On the other hand, commerce in an electronic environment has the features of international trade: uncertainty as to choice of law and jurisdiction, quality, performance, access to redress and enforcement and is also bedeviled with the challenge of doing business with anonymous parties.

2.1.1 Effect of regulation

As a global phenomenon, the electronic environment is not confined to a particular geographic location. This borderless "workplace", which is now the hub of business, is not subject to a universal law or administration but may be accessed universally. The concomitant effect is that many users of the internet are faced with the frustration of resolving serious legal issues if and when they arise, and that is where the role of the law comes into play. According to Susskind,[2] "the law is at the heart of our personal lives, it is the lifeblood of the commercial world and it is central also to our national security". With or without cohesive regulation, activities on the WWW will continue to grow exponentially in the face of security and legal challenges. These challenges call for an established body of internationally accepted laws or regulations for the

1 Amro (2016) 20 *Vindobona Journal of International Commercial Law & Arbitration* 10.
2 Susskind *The Future of Law* 11.

protection of consumers. The e-commerce consumer is, therefore, currently at a disadvantage when compared to the conventional commercial consumer. It is this disadvantage that is sought to be cured by the development of a comprehensive set of principles and rules of law for their protection.

E-commerce is permeated by global IT. The widespread use of IT is unprecedented; it is used for business, entertainment, security, and research, to name but a few areas. For many, the use of electronic devices has become a habit. The electronic environment begins with electronic devices or gadgets such as cell phones or personal computers (PC), and then migrates to the networking of computers which is referred to as the internet and related applications. Series of activities take place in this electronic world, including private communications and transactions, social communications, and, most importantly for present purposes, commerce.

These activities spur up legal rights, obligations, and liabilities. The effects of legal rights, obligations and liabilities can be grave and far-reaching for the user, particularly when they take place in an unregulated or under-regulated environment.

2.2 Information technology and computers

2.2.1 Information technology

IT has been a decided boon for the use of computers in e-commerce. IT is

> the acquisition, processing, storage, and dissemination of audio, graphic, textual, and numerical information by a microelectronics-based combination of computing and telecommunication technologies.[3]

According to Wouters[4] "the term information technology first appeared in a 1958 article published in the *Harvard Business Review"*, where authors, Leavitt and Whisler, remarked that "the new technology does not yet have a single established name, we

[3] Longley and Shain *Dictionary of Information Technology* 164.

[4] Wouters "The History of information technology – spine theme demo" (2017) available at www.spine.paulwp.com (date of use: 18 October 2020).

shall call it *information technology*."[5] Some new areas of IT are next generation web technologies such as bioinformatics, blockchain, cloud computing, global information systems, smart contracts, data analytics, large-scale knowledge bases, etcetera.[6]

2.2.2 Defining a computer

A computer is simply defined as an electronic device which processes information under the control of stored basic instructions.[7] The first set of computers date back to 1936 with the invention of Konrad Zuse's first freely programmable computer.[8] There are various types of computers including the PC,[9] desktop,[10] laptop,[11] palmtop, commonly known as personal digital assistant (PDA),[12] and workstations for specialised group of tasks, such as three dimensional (3D) graphics.[13] Servers,[14] especially with their powerful processors, and large hard drives[15] are optimised computers. There are also mainframes,[16] mini computers,[17] super-computers,[18] and wearable computers.[19]

---

5 Leavitt and Whisler *(*1958) *Harvard Business Review* 11 cited in Wouters "The History of information technology – Spine theme demo" (2017) available at www.spine.paulwp.com (date of use: 18 October 2020).

6 See Denning *et al* (1989) 32 *Communications of the ACM* 12.

7 Adebisi *Fundamentals of Computer Studies* 1.

8 Konrad "ZI Konrad Zuse Internet Archive" available at http://zuse.zib.de (date of use: 24 May 2019).

9 NOUN *Introduction to Computers* CIT 104 20.

10 Frost and Sullivan 2015 "Desktop Virtualisation: Implementing the Workplace of the Future, Today" 5-6 available at www.fujitsu.com (date of use: 18 August 2020).

11 *The Tech Terms Computer Dictionary* available at http://techterms.com (date of use: 13 August 2020).

12 Ringdon ed Dictionary of Computer 903.

13 Microsoft *Computer Dictionary 574*.

14 Ringdon ed *Dictionary of Computer* 1136.

15 Ayeni et al *Computers in Society* 11.

16 IBM *Dictionary of IBM & Computing Terminology* 53.

17 Information Systems Analysts and Consultants *Information Technology Terminology* 34.

18 Onifade "History of the Computer" 7 available at www.ethw.org/pdf (date of use: 16 August 2020).

19 These are computer applications which are integrated into clothing and personal items see Microsoft Computer Dictionary *562*.

2.2.2.1 Uses of Computers

(a) Electronic devices

In essence, a computer is an electronic device[20] or appliance. There are, however, other electronic appliances which function as a computer in disseminating information and which are used as internet conduits. These, too, therefore, serve as e-commerce tools. These electronic appliances include mobile phones, pagers, i-pads, and some devices that have adopted newer technologies, such as drones.

(b) Computers can be used as wireless devices

Wireless devices could be fixed wireless,[21] mobile wireless and data services,[22] portable wireless,[23] and infrared radiation (IR) wireless.[24]

2.2.2.2 Computers and internet networks

For computers to communicate, they need to network. The use of computer networks across all facets of economic and social life today is widespread due to convenience and access to the internet.[25] Networks can be used to transfer information between computers even when they use different operating systems.[26] A network can also be used to send data to remote storage devices and printers.[27] Generally, networks provide an inexpensive way to interconnect any number of systems and make communication and sharing of data quick and easy. There are two main categories of networks in use: the Local Area Network (LAN); and the Wide Area Network (WAN).[28]

---

20 Electronic means "relating to technology having electrical, digital, magnetic, wireless, optical, electromagnetic, or similar capabilities" see the United States Uniform Electronic Transactions Act, 2002 (UETA) s 5.

21 *Webster's New World Telecom Dictionary Online-Your Dictionary*, available at www.yourdictionary.com (date of use: 18 August 2020).

22 Wireless Technology Terms Glossary and Dictionary available at www.anritsu.com (date of use: 18 August 2020).

23 NOUN *Wireless Communication* 1 CIT 655 9.

24 Ibid.

25 Adebisi *Fundamentals of Computer Studies* 36.

26 Ibid.

27 Ibid.

28 Ayeni et al *Computers in Society* 11.

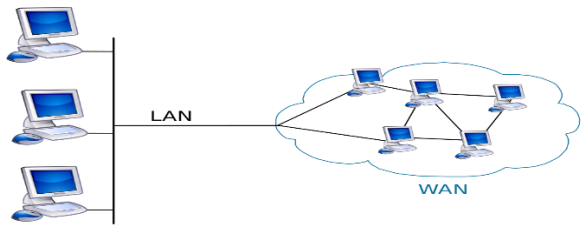
(a) Local Area Network

A LAN is a network for "linking private telecommunications equipment, personal computers and workstations to share data, devises or programmes within a single building or department."[29] While a Metropolitan Area Network (MAN) refers to LANs linked between buildings in the same area.[30] A MAN is between the LAN and WAN in terms of size.[31]

(b) Wide Area Networks

A WAN is a telecommunication or computer network which extends over a large geographic area. It is a computer network technology used to transmit data over long distances.[32] It can also be defined as a computer network spanning, regions, countries, or even the world.[33]

Diagram 2.1 WAN



Design from Pinterest available at https://www.pinterest.ca (date of use: 03 July 2020).

WAN functions as the internet[34] and the internet could be regarded as a global network of connected LANs and WANs.

29 Available at www.dictionary.com (date of use: 05 March 2020).
30 Asafe, Adebayo and Olalekan *Data communications* 32.
31 Information Systems Analysts and Consultants *Information Technology Terminology* 31.
32 *Webster's New World Telecom Dictionary Online*-Your Dictionary, available at www.yourdictionary.com (date of use: 18 August 2020).
33 Forouzan *Data Communications and Networking* 14.
34 Groth and Skandier *Network + Study Guide* 4.

2.2.2.3 World Wide Web (WWW)

The WWW

> is the total set of interlinked hypertext documents residing on (HTTP) servers all around the world. Documents on the World Wide Web called pages or web pages, are written in HTML (Hypertext Markup Language) identified by URLs (uniform resource locators) that specify the particular machine and pathname by which a file can be accessed.[35]

2.3 The internet

The internet is closely related to the invention of the computer. That explains why it is imperative that tolink the role of computers and electronics and the evolution of IT, to the emergence of the internet.

2.3.1 Origin of the internet

The story of the internet began with the launching of "Sputnik which was the first man-made satellite in 1957 by the then Soviet Union (the USSR)".[36] The US proactively decided to create the Advanced Research Projects Agency (ARPA) in 1958 in order to gain a technological edge[37] with emphasis on computer networking.[38] In the 1970s the ARPA was renamed the Defence Advanced Research Projects (DARPA) but this was reverted to ARPA in 2014.[39] Decades ago computers were enormous and took up large spaces however; they only had "a fraction of the power and processing capacity of a modern personal computer (PC)"[40] and could not network.[41] The ARPA had to hire

---

35 Microsoft Press *Microsoft Computer Dictionary* 574.

36 History.com "Sputnik launched" available at www.history.com (date of use: 30 July 2020).

37 BBN Inc, *A History of the ARPANET: The First Decade* 2; see also National Academics of Sciences, Engineering & Medicine *An Assessment of ARPA-E* 2.

38 BBN Inc, *A History of the ARPANET: The First Decade* 2.

39 See Internet – Guide "ARPA/DARPA: Contribution to the creation of the internet" available at www.internet-guide.co.uk (date of use: 26 July 2020).

40 "How did the internet start?" available at https://computer.howstuffworks.com (date of use: 30 July 2020); see also "Invention of the PC" available at https://www.history.com (date of use: 30 July 2020).

41 Garners "Early Popular Computers, 1950-1970" available at www.ethw.org (date of use: 17 August 2020).

the company Bolt, Beranek and Newman (BBN) whose task was to develop protocols that would enable computers to network.[42]

This was achieved when four nodes (computers) could connect to the ARPA network (ARPANET)[43] and this has become a reference point in the history of the internet.[44] The ARPANET was a US government-sponsored project under DARPA, a branch of the US Department of Defence.[45] They had computers at research centers and some private institutions[46] and made designs of internet protocols which are still in use today.[47]

2.3.2 Definition of the internet

"The internet is a collection of networked computer systems that span the entire globe";[48] it is a network of computer networks.[49] Computers communicate using the HTML common language[50] with the help of rules or protocols. The internet

> also relies on a huge infrastructure of routers, network access points (NAPs), and computer systems, in conjunction with satellites, miles of cable, and hundreds of wireless routers that transmit signals between computers and networks.[51]

The name "internet" derives from the phrase "interconnected networks."[52] Since its inception in about 1969, the internet has grown to hosting any sort of properly

---

42 Alperin et al BB&N Inc *A Case History of Transition* (2001) 43 available at www.web.mit.edu (date of use: 17 August 2020).

43 BB&N Inc, *A History of the ARPANET* (chapter 2) 22.

44 On arguments on the history of the Internet see Peter "So, who really did invent the internet?" available at www.nethistory.info (date of use: 13 August 2020).

45 Alperin et al BB&N Inc *A case History of Transition* (2001) 40.

46 BB&N Inc, *A History of the ARPANET* (chapter 3) 91, 95.

47 Ibid at (chapter 2) 10-22.

48 Downing and Covington *Dictionary of Computer and Internet Terms* 243; Margolis *Random House Dictionary* 283.

49 Smith *Internet Law and Regulation* 1. In *Religious Technology Center v Netcom On-line Communication Services Inc, 907 F. Supp. 1361 (1995) US District Court, California*, the court cited the internet as the "set of all interconnected IP networks" fn 2 1383.

50 Ayeni *et al Computers in Society* 175.

51 Strickland "Who owns the internet?" available at https://computer.howstuffworks.com (date of use: 18 August 2020).

52 Bourgeois and Bourgeois *Information Systems and Beyond* (Chapter Five) available at https://bus206.pressbooks.com (date of use: 17 August 2020).

interfaced device and spreading across millions of users all over the world.[53] By simply connecting a modem or any wireless device to a computer, the connected computer forms part of the network of an Internet Service Provider (ISP) which enables internet access. The ISP to whose service the user subscribes connects to and forms part of a larger network; which is the internet.[54]

Although there are different networks, there is no single or main controlling network. For example, in Nigeria the predominant networks are Mobile Telephone Network (MTN) Nigeria, Globacom Limited (Glo), Etisalat, Airtel, and a few others.[55] These network industries or organisations are linked to dedicated backbones which connects areas where they have a point of presence (PoP) on the internet. It is through the PoP that users in a particular area can access the organisation's network through the use of a Wi-Fi or telephone number.[56] These networks connect to each other through the NAP; while the Domain Name System (DNS) server and other powerful servers assist in the process by sending information online around the world in milliseconds![57]

2.3.3 Internet tools

The internet cannot function without backbones and routers; these are referred to as internet tools and are discussed below.

(a) Internet backbones

The first high-speed or backbone was a Transmission System 1 (T1) line[58] that operated at a very high speed.[59] The T1 line connects a service provider to the

53 Zittran (2006) 119 *Harvard Law Review* 1975-1976.

54 Tyson "How Internet Infrastructure Works" 2001 available at http://computer.howstuffworks.com (date of use: 26 August 2020).

55 Techviews "Top Nigerian Mobile Network Operators" available at https://techviews.com.ng (date of use: 07 October 2020).

56 Rouse "Point-of-presence" available at www.searchnetworking.techtarget.com (date of use: 07 October 2020).

57 Ayeni *et al Computers in Society* 175.

58 According to Pratt, "a T1 internet line is a fiber optic internet line that carries data at a moderately fast rate of 1.44 megabits per second or 192,000 bits per second." It is used for keeping several computers connected at high internet speed, Pratt (2013) "How fast is a T1 internet line and what is it?" available at https://www.business.org (date of use: 19 August 2020).

client.[60] It is through the T1 backbones that data traffic is delivered to customers across different backbones which are owned and operated freely by different companies.[61]

(b) Internet routers

Internet routers are specialised devices used in sending messages across networks.[62] A router's function is distinct: firstly, it prevents information from going to the wrong path; and secondly, it ensures that it reaches its intended destination.[63] In performing these two functions, the router deals with separate networks and protects them from each other to ensure that data traffic from one network does not spill to another network.[64]

(c) Internet protocol: IP addresses

The internet works because of a system of rules called protocols. These protocols are in the form of addresses known as Internet Protocol (IP) Address. These addresses are unique to computers that are connected on the internet. By following these protocols computers can send information across the network to other computers.[65] However, due to the difficulty of remembering numbers, words are used for identifying sites in place of numbers.[66] These words are called "domain names" such as www.unisa.ac.za. The "WWW" stands for World Wide Web and "UNISA" which is the host name is a second level domain (SLD) name, while "ac.za" is the country code top level domain (ccTLD) name. Each time a domain

59 NSFNET "About NSFNET" available at www.nsfnet-legacy.org (date of use: 29 May 2020).
60 Techopedia "What is a T1 line? available at https://www.techopedia.com (date of use: 29 May 2020).
61 Kende (2003) 11 *Commlaw Conspectus* 25.
62 Moore "Routers" (2017) 2 available at https://www.researchgate.net/publication/317057644 (date of use: 18 August 2020).
63 Ayeni *et al Computers in Society* 175.
64 Buecker et al *IBM Security Solutions Architecture for Network* 114.
65 WhatisMy IPAddress.com "Without IP Addresses, the internet would disappear" available at www.whatismyipaddress.com (date of use: 06 October 2020).
66 American Registry for Internet Numbers (ARIN) IP Addresses and Domain Names available at www.arin.net (date of use: 18 August 2020).

name is used, the internet DNS server translates the words in the domain name into a machine-readable IP address.[61]

2.4 An outlook on electronic transactions

Electronic transactions could be statutorily classified or interpreted in literal terms. Literally, all transactions or communications exchanged by electronic means qualify for legal protection. Statutorily, however, e-transactions are defined differently in various jurisdictions with some definitions being broader than others. Whatever definition is provided by law, determines the parameters within which the recognised form of e-transaction (whether commercial or not) may be regulated. In some legislative enactments or Acts, the terms e-transaction and e-communication are used together. The Australian Act, [62] for example, makes provision for the use of both "e-communication" and "transaction" as follows.

The Australian Electronics Transaction Act (ETA) defines e-communication as,

> (a) communication of information in the form of data, text or images by means of guided and/or unguided electromagnetic energy; or
> (b) communication of information in the form of speech by means of guided and/or unguided electromagnetic energy, where the speech is processed at its destination by an automated voice recognition system.[63]

While transaction is defined as:

> (a) Any transaction in the nature of a contract, agreement or other arrangement; and
> (b) Any statement, declaration, demand, notice or request, including an offer and the acceptance of an offer, that the parties are required to make or choose to make in connection with the formation or performance of a contract, agreement or other arrangement; and
> (c) Any transaction of a non-commercial nature.[64]

61 Ibid.
62 Electronics Transactions Act 162 of 1999 (as amended) s 5, (ETA).
63 ETA s 5(1).
64 Ibid.

In the same vein, the South African Electronic Communications and Transactions Act (ECTA)[65] define both terms similarly. Section 1 of the ECTA defines transaction as a "transaction of either a commercial or non-commercial nature, and includes the provision of information and e-government services"; while e-communication is defined as "communication by means of data messages".[66] The relationship between the two terms is that e-communications have legal validity in whatever form, and that transactions formed by e-communications are to that extent also recognised.[67]

The use of both terms in national legislation notwithstanding, what calls for attention is the scope of the various enactments and whether or not a particular enactment provides for both commercial and non-commercial transactions or is limited to commercial transactions. This dichotomy in the definition of e-transactions is noteworthy as not all e-transaction-legislation operates within the same scope.

2.5 Electronic commerce: An offshoot of electronic transactions

E-commerce is an offshoot of the commercial aspect of e-transactions. It includes m-commerce and forms part of electronic business (e-business). E-business is an evolving term which has gradually worked its way into the electronic lexicon. In addition to buying and selling on the internet, e-business is broadly defined to include "conducting all kinds of business online such as servicing customers, collaborating with business partners, delivering e-learning, and conducting electronic transactions within an organisation."[68] E-commerce, on the other hand, has been defined "as the conduct of commerce in goods and services with the assistance of e-communications and telecommunication-based tools".[69] E-commerce relies on transactions between

65 Electronic Communications and Transactions Act 25 of 2002 (ECTA) s 1.
66 Ibid.
67 ECTA ss 11(1) and 22(1).
68 Turban *Electronic Commerce* 7; see also Okoli and Mbarika "A framework for accessing e-commerce" 5.
69 Clarke "Electronic commerce definitions" available at www.rogerclarke.com (date of use: 02 July 2020).

businesses, groups, and individuals using the internet or intranets.[70] In simple terms, e-commerce is generally taken to be the sales feature of e-business.[71]

2.5.1 Electronic commerce defined

E-commerce entails the electronic purchase of goods or services using virtual stores or electronic web (e-web) stores[72] rather than brick-and-mortar retail shops. The World Trade Organisation (WTO) defines e-commerce as the "production, distribution, marketing, sale, or delivery of goods and services by electronic means".[73] In essence, e-commerce is conducted without physical presence or the use of paper-based communication but by means of an EDI and other means of communication.

In e-commerce the term "commercial communication" features regularly. The E-commerce Regulations[74] of the UK define a commercial communication as:

> a communication, in any form, designed to promote, directly or indirectly, the goods, services, or image of any person pursuing a commercial, industrial, or craft activity, or exercising a regulated profession.

However, in terms of the Regulations, the following will not constitute commercial communications

(a) information allowing direct access to the activity of that person including a geographic address, a domain name or an electronic mail address; or
(b) information relating to the goods, services or image of that person provided that it has been prepared independently of the person making it (and for this purpose, a

---

70 Ibid. Intranets are networks used within private establishments with the aid of internet protocols to connect to the internet or to other computers within the establishment. The "intranet could be either a local area network (LAN) that connects computers in a relatively small area, like a building, or a wide area network (WAN) which covers a large geographical area. Intranets are usually hidden from public access by the use of protective firewalls", see Buys and Rothmann "Internet Law and Regulation" 18.

71 For further discussion on e-business and web stores see Turban *Electronic Commerce* 5.

72 The terms, e-web stores, online store, virtual malls, or web shops are used to refer to various online trading platforms and they mean the same thing.

73 WTO "Electronic commerce" (2017) available at www.wto.org/english/thewto_e/ecom (date of use: 20 June 2020).

74 The Electronic Commerce (EC Directive) Regulations 2002 UK 2002 No 2013 s 2(1).

> communication prepared without financial consideration is to be taken to have been prepared independently unless the contrary is shown).[75]

Lodder and Kasperson[76] define e-commerce as

> any business transaction concerning goods and services, including relating commercial activities, where participants are not at the same physical location and communicate through electronic means.

E-commerce is thus distinct from commercial trade or transactions conducted without the use of e-communication. To capture the definition of e-commerce more aptly, it is useful to consider the earlier WTO's definition of e-commerce in terms of which e-commerce is carried out by electronic means. The distinction, therefore, is that e-commerce involves trade, business, or commerce conducted outside of the traditional means of trading such as physical contact, mail, or newspaper advertisements, and relies solely on electronic means.

E-commerce could therefore be defined as a trade system between parties where the parties rely solely on electronic means of communication for the entire or major part of, the process of trading without any form of face-to-face contact,[77] although there could be physical delivery of goods. E-commerce excludes any form of physical or direct contact and includes any form of e-communication. In Buckley's[78] view, e-commerce is defined as:

> a means of conducting transactions that, prior to the evolution of the internet as business tool in 1995, would have been completed in more traditional ways – by telephone, mail, facsimile, proprietary electronic data interchange systems, or face-to-face contact.

Suffice it to say that e-commerce can actually be conducted by some of the traditional means identified in Buckley's definition, provided that the trade or commerce is

---

75 Section 2(1) Electronic Commerce (EC Directive) Regulations, 2002.
76 Lodder and Kasperson *e-Directives* 1-9
77 Physical contact between the parties makes the transaction more of a distance or conventional trade.
78 US Department of commerce *The emerging digital economy* 1.

conducted solely by means of an electronic tool or telecommunication facility and without face-to-face contact.

2.5.2 Types of electronic commerce

The classification of types of e-commerce activity is based on who the parties to the transaction are. The activity may be business-to-business (B2B), where business is conducted online between corporate entities.[79] It should be noted that from the definition of a consumer in paragraph 2.6 parties to this form of e-commerce will not be protected under e-commerce consumer-protection laws or rules. E-commerce could also be classified as business-to-consumer (B2C); [80] business-to-administration/government (B2A/G);[81] or consumer-to-consumer (C2C)[82] – examples of this latter group are found in auction sites such as eBay.com.[83] Another form of e-commerce could be government-to-businesses (G2B)[84], or government-to-consumers (G2C). [85] The research interest here is on B2C; consumer-to-consumer is not considered in details as both parties act on an equal level, although it could be argued that a consumer acting as a supplier must, for purpose of that trade, bear the responsibilities of a supplier.

2.5.3 Forms of electronic commerce trade

Through e-commerce, varieties of trade take place by way of online shopping. The different offerings include electronic retailing (e-tailing), subscription sites, mobile

79 Lodder and Kasperson *e-Directives* 4.

80 A transaction between a business and a consumer, see Drigas and Leliopoulos (2013) 4/4 *International Journal of Knowledge Society Research* 1.

81 Transactions where business provides an online service to government; see Shahjee (2016) 4/27 *SRJIS* 3135.

82 The transaction wherein there is reliance on a third party to act as intermediary for the transact-tion, see Gupta (2014) 4/1 *International Journal of Computing and Corporate Research* 2.

83 Lodder and Kaspersen *e-Directives* 4.

84 The transaction wherein e-governance tools are used to aid the business community; see Shahjee (2016) 4/27 *SRJIS* 3135.

85 Electronic interaction between government agencies and private businesses, Raisinghani "Key factors and implications for e-government diffusion in developed economies" 2305.

application sales, online banking, travel agencies, digital goods stores, electronic book purchases, online auctions, and the procurement of various services through the web, etcetera.

2.5.3.1 Online shopping

Online shopping was invented in 1979 by Michael Aldrich by connecting a modified domestic television (TV) to a real-time transaction-processing computer using a domestic telephone line.[86] In March 1980 consumers could complete transactions online through the Redifon's Office Revolution and videotext technology.[87] These systems predate the internet, the WWW, and Microsoft disk operating systems (MS-DOS), and were pioneered in the UK.[88]

2.5.3.2 Electronic retailing

Electronic retailing (e-tailing) also known as "virtual storefronts," is the practice of listing products and their histories for sale in a catalog format on a website.[89] Some e-tailing sites (perhaps most notably Amazon.com) take this a step further to aggregate numerous smaller stores into a unified system akin to a "virtual mall".[90]

2.5.4 Electronic commerce technologies

Before the prevalent use of the internet and the consequent promotion of commercial trade online (e-commerce), other technologies such as virtual private networks (VPNs); EDI and EFT[91] were already in use between businesses.

---

86 Aldrich (2011) 33/4 (Oct-Dec) *Annals of the History of Computing* 57.
87 Aldrich (2011) 33/4 (Oct-Dec) *Annals of the History of Computing* 60.
88 Aldrich *Video-Key to the wired City* 672.
89 *Barrons Dictionary of Marketing Terms* available at www.allbusiness.com/barrons_dictionary (date of use: 18 August 2020).
90 Financial Dictionary "Virtual Mall" available at https://financial-dictionary.thefreedictionary.com (date of use: 20 June 2020).
91 Tarasewich, Nickerson and Warkentin (2002) Seventh Americas Conference on Information Systems 437.

2.5.4.1 Electronic data interchange

The EDI "is a system of e-communications between commercial parties where the communication takes place over a closed system and are governed by a set of previously agreed contracts."[92] EDI is essentially online communications between business partners who have on-going business relationships within an agreed framework.[93] In addition, businesses can exchange electronic documents (e-documents) through EDI using automated computer applications.[94] EDI can also be used to send orders to warehouses and generate invoices from such orders.[95]

EDI was predicted by some writers to be the new tool for global business.[96] There are, however, major differences between EDI and the internet. First, EDI uses pre-determined forms and formats, whereas communication on the internet takes place freely. Secondly, the EDI is based on an underlying interchange agreement between established and select business partners, whereas the internet is open to everyone for sales and services without a prior relationship or arrangement being required. Finally, while the EDI takes place without any human intervention, internet contracts sometimes involve some form of human effort.[97] In early 1990s, it was assumed that EDI would be the future mainstay of e-trade but all that changed with the evolution of the internet.[98] Although EDI is still used between businesses,[99] its functions are now largely performed by the internet.

---

92 UNCITRAL Model Law art 2 (b).

93 See further, Van der Merwe et al *Information and Communications* 150; Eiselen (1995) 7 *SA Merc LJ* 1-2; Mann and Winn *Electronic Commerce* 332, 343; Reed & Angel *Computer Law* 224-5; Pistorius (2002) 35 *CILSA* 138-139.

94 Hance & Balz *Business and Law on the Internet* 164; Chandler (1998) 22 *Tulane Maritime Law Journal* 464.

95 Techterms "EDI" available at www.techterms.com (date of use: 15 October 2020).

96 Coetzee (2004) 15/3 *Stell LR* 501-2; Meiring "Electronic Transactions" 82-3; Faria (2004) 16 SA *Merc LJ* 529; Geist *Internet Law in Canada* 544-5.

97 Pistorius (2002) 35 *CILSA* 9.

98 Mann and Winn *Electronic Commerce* 333-6; Eiselen (1995) 7 *SA Merc LJ* 1-2; Walden *EDI and the Law* xi-xii, 1-2; Baum MS & Perrit *Electronic Contracting* 1-7.

99 Lloyd *Information Technology Law* 423-4.

2.5.4.2 Virtual private networks

Apart from closed network systems such as the EDI, VPNs also allow users to communicate over the internet based on agreed trade regulations.[100] Businesses use VPNs to communicate across multiple locations so that a business can send data to its branches in different parts of the world by using a VPN with an encrypted connection (similar to a secure intranet) over the internet.[101] With this form of arrangement, individual users may maintain a VPN account with their company which allows them to access their office computers remotely.

2.5.4.3 Electronic fund transfer

EFT is the transfer of funds by various electronic means, including the use of mobile phones and computers. It was part of the early e-commerce applications which were developed in the early 1970s.[102]

2.5.5 Mobile commerce

M-commerce is a commercial transaction carried out through "…a mobile telecommunications network".[103] M-commerce can fulfill most of the functions of e-commerce; it is used for purchases, downloading of content, and accessing information on the mobile screen. There are numerous mobile applications designed specifically for mobile devices. These applications are used to access weather information, play games, determine the location of information, make payments – the list is endless. Mobile phones perform virtually all functions of e-commerce unless a specific computing functionality is required to complete the transaction.[104] Some of the strains observed in the use of mobile devices for m-commerce have been identified to

100 Stewart *Network Security* 79.

101 Kajal, Saini and Grewal (2012) 2/10 *International Journal of Advanced Research in Computer Science and Software Engineering* 428.

102 Simplynotes "Origin of electronic commerce/history of e-commerce and evolution of e-commerce" available at www.simplynotes.in (date of use: 20 June 2020).

103 Antovski and Gusev "M-Commerce Services" 15 available at www.researchgate.net/publications (date of use: 09 February 2019).

104 OECD Policy Guidance for Addressing Emerging Consumer Protection 2-3.

include limited screens, low speed processor and small memory capacity.[105] To solve some of these technical issues there have been the adoption of new techniques, one of which is the wireless application protocol (WAP).The WAP "is an open, global specification that enables interaction between mobile terminals and internet services."[106]

Inherent in m-commerce transactions are challenges of misleading advertisements, for instance, in m-commerce, an advertisement through a mobile view could contain terms, notifications, disclaimers, or charges in very small print which the m-consumer may not be aware of, but on the basis of which he or she would be liable. Furthermore, there are cases of exploitation of minors especially through overconsumption which could occur through voting sites.[107] There are bogus voting applications that apply special charges (usually indicated in unintelligible print) which result in unexpected bills for consumers. To streamline such challenges, mobile operators should restrict certain adverts that go to devices operated by underage consumers, and set a monthly bill limit to minimize such occurrences, failing which the child's parent or guardian should not be held liable for the additional cost. Again, notices of bills that exceed certain limits at a particular time may be sent to the parents or guardians. Age-restriction tools could also be applied, notwithstanding that some children may circumvent the tools. There should be awareness and education of both parents and children on the use of mobile devices by children, and existing rules protecting children on the internet should be adapted to the mobile environment. Parents should be educated to activate filtering devices to block internet access to inappropriate content on their children's mobile devices. Purchases could also be blocked on children's devices other than those from sources which are approved by the parents or guardians. Parents or guardians may further need to understand the technologies installed on their children's devices for which no one can be held liable – for example, Bluetooth.

105 Aithal *Mobile Commerce* 7.
106 Pessi "Exploring mobile e-commerce" 2.
107 OECD Policy Guidance for Addressing Emerging Consumer Protection 3.

M-consumers do suffer loses when they engage in transactions in locations where they are geographically blocked or restricted. Unfortunately, this form of restriction may not be apparent to consumers especially m-consumers in view of the limited screen of a mobile device. The consequences of notifications on geographic restrictions are that any subsequent grievance arising from such a transaction would not be addressed if it is a transaction falling outside the supplier's specified location.[108] Furthermore, issues may arise from a complex chain of contracts where, for example, purchases of mobile tickets for bus, theatre, or television subscription are made telephonically with anonymous vendors.[109] More complex problems could further arise where bills for mobile commerce transactions are billed to mobile subscribers by the consumer's mobile operator on behalf of the vendor of the goods or services through mobile wallets s or credit cards.

The problem of unsolicited communications is not uncommon in m-commerce in fact there could be deductions from the consumer's account, to pay for unsolicited subscriptions to which the consumer may not have consented. Some of these subscriptions do not come with opt-out options in the first few days of the service,[110] thus holding the consumer to ransom until a customer-care line is called to intervene. Also associated with the use of mobile devices is theft of the device which could lead to identity theft.[111] Mobile devices are easily accessed especially with Google saved passwords and can therefore be used for quick purchases in cases where the mobile phone also acts as an electronic wallet. In order to minimiz

---

108 In addressing the disadvantage which a consumer may face as a result of geographical blocking or geo-blocking the EU set up a regulation known as Regulation (EU) 2018/302 of the European Parliament and of the Council of 28 February 2018 on addressing unjustified geo-blocking and other forms of discrimination based on customers' nationality, place of residence or place of establishment within the internal market and amending Regulations (EC) No 2006/2004 and (EU) 2017/2394 and Directive 2009/22/EC *OJL* 601, 2.3.2018, 1-15. The Regulation seeks to provide opportunities for consumers in the EU Member states to trade without restrictions within the EU.

109 Niranjanamurthy et al (2013) 2/6 *International Journal of Advanced Research in Computer and Communication Engineering* 2362.

110 Akhigbe (2019) 6 *Benin Journal of Public Law* 196.

111 Niranjanamurthy et al (2013) 2/6 *International Journal of Advanced Research in Computer and Communication Engineering* 2360.

e the gains for criminals in possession of stolen mobile devices, it is important for vendors to confirm the identity of buyers through additional verification processes by sending confirmation to their e-mail addresses rather than the phone. That way, the consumer may continue to take charge of the m-commerce process in spite of the missing device. The use of credit limits on amounts that could be spent using a mobile device on a particular day or week could also limit theft through missing mobile devices.

The use of PIN codes to confirm each transaction and passwords to access mobile devices, would deter illicit use. Easy access to services through which the use of a device could be locked should be encouraged, as should easy access to deactivate stolen Subscriber Identification Module (SIM) cards. In addition, providers can set up special reporting lines for lost and stolen handsets where consumers could "key in" information to disable SIM cards. In Australia, if you report a lost or stolen mobile device to your mobile service provider, the phone will be blocked across the whole of the country. The service providers are able to do this by blocking the phone's unique 15-digit serial number, the International Mobile Equipment Identity (IMEI).[112]

To address privacy issues, there should be rules restricting the information (other than directory information such as name and telephone number) that mobile operators can disclose to third parties without the consumer's permission, including joint venture partners or independent contractors. Rules mandating conspicuous disclosure of a mobile operator's data-collection practices should also be considered.[113]

---

112 Amta "Lost and stolen phones" available at www.amta.org.au (date of use: 6 October 2020). This is possible since mobile handsets are equipped with a registered International Mobile Equipment Identification (IMEI) number, and mobile handsets using the code-division multiple access (CDMA) network technology are also equipped with an Electronic Serial Number (ESN), which, like IMEI is used to identify a unique mobile device. Each of the companies can place a bar on the SIM card or IC Chips and the IMEI via remote control to lock the handset and make it inoperable.

113 OECD Policy Guidelines for Addressing Emerging Consumer Protection at 6.

Based on associated issues with m-commerce, a consumer focus mystery-shopping survey conducted on the use of a mobile phone involving nineteen consumer organisations from eleven countries, found restrictive market choice, inadequate information disclosure, poor complaint handling and redress, problems with payments, insufficient advice on mobile security, and poor protection for under-age users from over consumption, to be major hurdles to m-commerce.[114]

2.5.6 Electronic commerce products

The different forms of e-commerce transaction notwithstanding, e-commerce is largely categorised as the sale of goods and services. Intangibles such as data, digital goods, as well as software, are classified as services.[115] Electronic services (e-services) have been defined as "one prominent application of utilizing the use of information and communication technologies in different areas."[116] Goods on the other hand are defined as physical or tangible items that satisfy human wants or needs.[117] Such items will include computers, printed books, clothing, and other physical objects such as cars, clothes, household utensils, and other tangible items.

---

114 Kisielowska-Lipman 2009 *Consumer Focus* 20.

115 Generally, a service is the intangible equivalent of economic goods. This is particularly so as software is delivered for its electronic functionality see Scupola, Hente and Nicolajsen (2009) 1/3 *International Journal of E-services & Mobile Applications* 11.

116 Definitions.net "What does e-services mean?" available at www.definitions.net (date of use: 20 June 2020). E-services are generally in the nature of banking, travel booking services, online entertainment and so on. Furthermore, services can be in the form of a "service contract." A service contract is "a contract for services such as time, expertise, and effort instead of goods" see The Law Dictionary "What is service contract?" available at http://thelawdictionary.org (date of use: 20 June 2020).

117 *Business Dictionary* available at www.businessdictionary.com (date of use: 05 September 2020). While the distinction between certain goods and services is not always clear, some products clearly stand out as goods. A "product" can be further defined as a thing produced by labour or an industrial process *Cambridge Dictionary* available at www.dictionary.cambridge.org (date of use: 15 September 2020). It must, however, be noted that the sale of fixed assets such as a house does not fall within the scope of most e-transaction or e-consumer protection laws, See, for instance, art 3(3e) Consumer Rights Directive; s 2(2)(e) E-transactions Bill, 2017 (Nigeria).

2.5.7 Electronic commerce and distance trade

A look at e-commerce from the perspective of e-transactions and consumer protection laws would show that the concept of e-commerce hinges on trade by means of alternatives to physical contact and paper-based communication. With this in mind, it is safe to claim that a trade conducted by means of physical mail or printed advertisement without any physical contact, but based on faceless communication, will qualify as distance trade as opposed to e-commerce. This brings us to the need to distinguish between e-commerce and distance trade.

2.5.7.1 Distance trade

Distance trade refers to contracts concluded at a distance. Distance trade includes any contract concerning goods or services between a supplier and a consumer by the sole use of distance communication for the entire period of the contract. Such sales or services must be between the buyer and seller without the parties being physically present.[118] Likely means of communication would include the internet, telephone, fax, mail orders,[119] newspapers, radio, television, or letters.

2.5.7.2 Distinction between e-commerce and distance trade

While e-commerce and distance trade are both conducted without physical contact between the parties, the underlining difference is that e-commerce must be conducted by electronic means in addition to, or in the absence of, other means of distance communication. Therefore, trade by means of catalogues and unaddressed or

---

118 Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament, *OJL* 304, 22.11.2011 64-88 (CRD) art 2(7). In the course of this research attempts were made to study concepts in distance trade from regions outside of the EU, the outcome left much to be desired thus narrowing most of the perspectives on distance trade to those of the EU.

119 See recital 20 CRD.

addressed printed matter, will not qualify as e-commerce, but will qualify as distance trade. Furthermore, e-commerce or e-transaction-specific regulations – for example, the EC Convention, the E-Commerce Directive, and similar regulations – will not apply to distance trade. Currently, distance trade is regulated in some jurisdictions under international trade laws,[120] while in the EU it is regulated by the CRD, which has been implemented in the UK by the Consumer Contracts (Information, Cancellation, and Additional Charges) Regulations 2013.[121] The CRD applies to both distance trade and e-commerce.

2.6 Formalities in electronic contracts

In order to formalise a contract agreement between parties with capacity to enter into legal relationship the basic elements of offer and acceptance must be present.[122] The online contract requires no less but that these elements are suited for the online environment. The principle behind a pre-offer is that it is an invitation not an offer in itself. The invitation can be withdrawn at any time without any obligation – it is, after all, only an invitation. The same rule applies online; the task is to identify what amounts to an invitation in an online environment. Offers on a website, or direct offers sent to e-mails and mobile phones, are all invitations unless the originator specifies that they also constitute offers. Where they are ordinarily invitations, it is the recipient who makes the offer when he or she indicates an interest in purchasing any of the items displayed. The supplier accepts the offer upon confirmation, and is expected to perform in terms of the contract. Where the initial invitation is also an offer, the recipient accepts the offer when he or she proceeds to accept the offer without any modification.

120 See for instance the "United Nations Convention on Contracts for the International Sale of Goods Vienna, 11 April 1980" where according to Flechtner the Convention had attracted over 70 countries as contracting states in 2009, available at www.legal.un.org (date of use: 10 October 2020).

121 The Consumer Contracts (Information, Cancellation, and Additional Charges) Regulations 2013 No 3134.

122 Sagay *Nigerian Law of Contract* 6.

The general rule is that every acceptance is preceded by an offer,[123] whereas not all offers are preceded by an invitation. Therefore, there must be a distinction between an offer and an invitation in order to create room for proper acceptance. This rule presupposes that an offer is made when it is communicated to the offeree, and, in an online environment, this happens when the communication leaves the information system of the offeror and enters the information system of the recipient.[124] Acceptance takes place when the acceptance reaches the offeror.[125]

The rules in offer and acceptance in e-contracts would seem to follow the postal rule but that would depend on the method of e-communication. Under the postal rule, immediately the acceptance has been dispatched by post, acceptance takes place irrespective of "if" and "when" it reaches the offeror. The postal rule applies in non-instantaneous communications. The question that is consistently asked in this context is whether or not a data message either on a webpage or sent by e-mail or text message is an instantaneous communication. The distinction in the rules governing both instantaneous and postal communications is that in instantaneous communications, an acceptance is effective upon receipt, while in postal communications, an acceptance is effective upon posting. If the latter is likened to an e-mail, then an acceptance becomes effective when it leaves the information system of the originator and enters the address system of the recipient in a condition that is accessible. Whether or not it has been retrieved by the recipient, is immaterial.[126]

Although there may not be much judicial pronouncement as to what rule applies to the place of acceptance in internet contracts, the decision of the court in *Entores Ltd v Miles Far Eastern Corp*[127] on acceptance sent by telex, is closely connected and gives some indication of the issues that may be raised before the courts. At issue here was

123 Kazeem *Electronic contract formation* 5.
124 See art 15 UNCITRAL Model Law and art 10 UN Convention on Electronic Contracts.
125 Sagay *Nigerian Law of Contract* 38.
126 See again art 15 UNCITRAL Model Law.
127 *Entores Ltd v Miles Far Eastern Corp* (1995) 2 QB 326 briefed from Rowland and Macdonald *Information Technology Law* 301.

the determination of the place of contract between the plaintiffs in London, and the defendant corporation in Holland. Lord Denning's analysis of what rule of acceptance should apply where an acceptance is communicated by telex, is engaging and is reproduced below.

> When a contract is made by post it is clear throughout the common law countries that the acceptance is complete as soon as the letter is put into the post box, and that is the place where the contract is made. But there is no clear rule about contract made by telephone or by Telex. Communications by those means are virtually instantaneous and stand on a different footing.
> The problem can only be solved by going in stages…Now take the case where two people make a contract by telephone. Suppose, for instance, that I make an offer to a man by telephone and, in the middle of his reply, the line goes 'dead' so that I do not hear his words of acceptance. There is no contract at that moment. The other man may not know the precise moment when the line failed. But he will know that the telephone conversation was abruptly broken off: because people usually say something to signify the end of their conversation. If he wishes to make a contract he must therefore get through again to make sure that I heard. Suppose next, that the line does not go dead, but is nevertheless so indistinct that I do not catch what he says and I ask him to repeat it. He then repeats it and I hear his acceptance. The contract is made, not on the first time when I do not hear, but only on the second when I do hear. If he does not repeat it there is no contract. The contract is only complete when I have his answer accepting the offer.
>
> Lastly, take the Telex, suppose a clerk in a London office taps out on the teleprinter an offer which is immediately recorded on a teleprinter in a Manchester office, and a clerk at that end taps out an acceptance. If the line goes dead in the middle of the sentence of acceptance, the teleprinter motor will stop. Then there is obviously no contract. The clerk at Manchester must get through again and send his complete sentence. But it may happen that the line does not go dead, yet the message does not get through to London. Thus the clerk at Manchester may tap out his acceptance and it will not be recorded in London because the ink at the London end fails or something of that kind. In that case, the Manchester clerk will not know of the failure but the London clerk will know of it and will immediately send back a message - 'not receiving.' Then, when the fault is rectified, the Manchester clerk will repeat the message. Only then is there a contract. If he does not repeat it there is no contract. It is not until the message is received that the contract is complete…
>
> My conclusion is that the rule about instantaneous communication between the parties is different from the rule about the post. The contract is only complete when the acceptance is received by the offeror: and the contract is made at the place where the acceptance is received.[128]

Following the same decision, in *Brinkibon Ltd v Stahag Stahl und Stahlwarenhandelgesellschaft mbH*[129] the parties negotiated the sale of steel bars and the buyer, an English company, accepted the offer by telex sent from London to

128 Ibid.

129 *Brinkibon Ltd v Stahag Stahl und Stahlwarenhandelgesellschaft mbH* (1983) 2 AC 34 briefed from Law Teacher available at http://www.lawteacher.net/cases (date of use: 15 October 2020).

Vienna. The issue was to determine the place where the contract had been concluded. The court held that the contract was concluded in Vienna.[130] The above notwithstanding, rules on acceptance through e-mail have not been clearly defined in courts.[131]

The argument for telex as an instantaneous communication is predicated on the fact that if the acceptance is not communicated, the offeree is in a position to know, and would therefore make another attempt to have the acceptance communicated. In the same way, the offeror would also be aware that an attempt has been made to reach him or her, but the communication may have failed, and he or she could then also attempt to re-establish communication. The e-mail system is quite different; here the offeree believes that the acceptance has been sent, especially where there is a 'sent' report, but the mail may have been delivered into a junk folder without the knowledge of the offeror. E-mails can also be misaddressed and sent to an unknown recipient where the originator does not pay attention.[132]

In Nigeria presently there is no specific legislation on when an e-message is deemed to have been received, and the conventional rules on offer and acceptance remain unclear in respect of electronic form of acceptance. The same technical challenge is faced in relation to the rule on place of contracting in that the general rule of the place where parties reside or do business, will not apply to e-transactions which in fact have "no place". Rather than the regular physical or geographic presence of the parties, the norm in internet cases is virtual presence. Virtual presence should be identifiable and accessible in order to satisfy the requirement of permanence, irrespective of the intangibility of the equipment or manpower that may be involved in the business at a specific location. For an internet-based business, a server serves all the functions of physical premises, utilities, and equipment. In order to meet the description of an

130 Ibid.
131 Wright (2008) *GIAC Legal Issues* 11.
132 See Akomolede (2008) 3 *PER* 6.

establishment as an online entity in a particular area, the server should, however, be located in that place for a reasonable period of time.[133]

Although some writers have argued that a server should not be treated as a business' establishment as it is possible to run a server based on programming, without human intervention.[134] It is believed, however, that the lack of human intervention does not change the status of a business establishment.[135] Suffice it to say that a business that does not have its own server, but leases a third party's server, cannot claim the place of establishment of the company that owns the server.[136] The business is only responsible for its data and software which is stored on the server and has no right to control the operation of the server.[137] Article 2 of the E-commerce Directive provides that the presence and use of the technical means and technologies required to provide a service, do not, in themselves, constitute an establishment of the provider or business. To show that a service provider is established as an entity in a given area, the E-commerce Directive provides that the service provider must have been effectively pursuing an economic activity in that location for an indefinite period.

From the foregoing, it is easy to deduce that a larger per cent of ISPs or vendors are third parties on a lease or service agreement with established service providers and, therefore, have no place of establishment. Determining their location must therefore be based on other factors, which should not primarily be dependent on the existence of the location of an information system or the domain name address of the parties.[138] This implies that in the absence of legislation, it will be more difficult to determine the location of parties to an internet contract concluded in an unregulated environment

133 Tang *Electronic Consumer Contracts* 69.
134 Reed *Internet Law* 182.
135 Tang *Electronic Consumer Contracts* 72.
136 OECD *Proposed Clarification of the Permanent Establishment Definition* para 3.
137 Tang *Electronic Consumer Contracts* 69.
138 Tang *Electronic Consumer Contracts* 69. Tang in page 14 particularly n 53 explains that IP addresses are unique and identify the location of devices through the use of special computer programmes. The IP addresses are presented by a series of numbers which professionals can read to identify the location of the device, although not all IP addresses are unique in the current technology.

such as Nigeria. Borrowing from established principles such as those in the UNCITRAL Model Law, the location of parties in an internet transaction can be inferred from the written address of the parties, their branch address, or, where they fail to provide any address, from their habitual place of residence.[139]

2.7 Electronic commerce concepts and the electronic commerce consumer

In conducting this research, defining a consumer has posed a challenge. Defining an e-commerce consumer is based, primarily, on identifying who qualifies as a consumer. The difference between a "regular" consumer and his or her e-commerce counterpart lies solely in the mode by which the transaction is performed – either in physical space or cyberspace. The definition of a consumer has been limited to the subjective requirement of "personal use" of the goods or services to which the transaction refers, and the restrictive personality of the consumer who must be a "natural" person or "an individual".[140] The Nigerian Federal Competition, Consumer Protection Act (FCCPA)[141] defines a consumer as "any person who purchases, or offers to purchase goods otherwise for the purpose of resale and includes any person to whom a service is rendered". The goods must not be purchased for the manufacture or production of any other product.[142] This definition is further supported by the E-commerce Directive which defines a consumer as "any natural person who is acting for purposes other than those of his trade, business or profession."[143] These definitions clearly exclude corporate entities from the definition of a consumer. However, the South African Consumer Protection Act (CPA)[144] extends the definition of a consumer to include a juristic person. The Act defines a consumer as a "person" and goes on to define a person to include juristic persons and public bodies. This inclusion is reflected in

139 UNCITRAL Model Law art 15 (4).
140 See Directive on Consumer ADR art 4(a).
141 Federal Competition, Consumer Protection Act 2019 (FCCPA) see s 170 for the definition of a consumer. The FCCPA was passed into law see "Buhari assents to Federal Competition, Consumer Protection Act 2019" 07 February 2019, available at www.vanguardngr.com (date of use: 07 October 2020).
142 FCCPA s 170.
143 E-Commerce Directive art 2(e).
144 Act 68 of 2008 s 1.

clause 1(f) of the Electronic Communications and Transactions Amendment Bill, 2012.[145]

2.7.1 Legal personality of a consumer

From the various definitions examined, a consumer should be a natural person and not a juristic person.[146] The whole concept of consumer protection is aimed at the protection of the buyer against the seller as the seller is perceived to be in a stronger bargaining position than the buyer.[147] This is reflected in paragraphs 23 and 24 of the Rome 1 Regulation[148] which provides for the protection of consumers being weaker parties to a transaction.

Harvey and Parry[149] observe, inter alia:

> In consumer transactions, unfair practices are widespread the existing law is still founded on the principle known as caveat emptor, meaning, let the buyer beware, the principle may have been appropriate for transactions conducted in village markets it ceased to be appropriate as a general rule now that the marketing of goods and services is conducted on an organised basis and by trained business executives. The untrained consumer is no match for the businessman who attempts to persuade the consumer to buy goods or services on terms suitable to the vendor, the consumer needs protection from the law.

Consumer protection laws generally do not apply to B2B transactions as businesses operate on an equal footing, with none of the parties needing greater protection than the other. Therefore, where the buyer is a business concern or a company, in most jurisdictions consumer protection law will not come to its aid. It should be noted that

---

145 Notice 08 of 2012 *Government Gazette* 35821. There is no indication that the bill has been passed into law see Ellipsis "Electronic Communications and Transactions Amendment Bill" available at www.ellipsis.co.za (date of use: 05 September 2020).

146 See, for example, s 170 FCCPA; s 1 SADC Model Law on Electronic Transaction and Electronic Commerce; art 2(e) E-Commerce Directive 2000; and s 102(a)(15) Uniform Computer Information Transactions Act 2002, US. Flowing from these sections of the law herein, the broader view of the definition of a consumer to include juristic persons under the CPA is not a widely accepted definition of a consumer.

147 Goldring J (1996) 2/2 *Journal of Computer Mediated Communication* 5.

148 Regulation (EC) 593/2008 of the European Parliament and of the Council of 17 June 2008 on the law applicable to contractual obligations (Rome 1) *OJL* 177, 4.7.2008 6-16.

149 Harvey and Parry *Consumer Protection and Fair Trading* 1 (this statement is credited to Senator Murphy, then Attorney-General of Australia, and was widely reported in Goldring (1974-75) 6 *Federal Law Review* 288.

where a legal person makes purchases for its employees for their personal use, it is the employee who is the final user and not the business. Viewed from this angle, consumer protection laws will be available to such an employee. Therefore, while businesses are not entitled to use consumer-protection measures, their employees may well be.

2.7.1.2 "Use" criterion in defining a consumer

Determining a consumer is also based on the use to which the product or service is put.[150] Therefore, where a natural person makes a purchase for business use, he or she will no longer qualify for consumer protection. It is immaterial whether at the time of purchase the goods were intended for personal use but were later converted for business. A case in point is that of *Benincasa v Dentalkit*,[151] where the plaintiff entered into a contract with the defendant in view of pursuing a trade, at a future date. The plaintiff later sought to be protected as a consumer when a dispute came up. The Court of the sixth Chamber held that with reference to article 13 of the Convention on Jurisdiction and the Enforcement of Judgements in Civil and Commercial Matters,[152] the plaintiff cannot enjoy the protection of the law as a consumer in respect of that particular contract which he had entered for the purpose of a future trade.[153]

Another scenario would be the partial use of goods purchased for both professional and personal use. The question is whether or not such a consumer should be entitled to protection as a consumer. In *Gruber v BayWa AG,*[154] the Austrian Supreme Court had to determine a number of questions brought before it by the court of first instance, among which was whether a "mixed" contract as the one concluded between the parties in the suit qualified as a consumer contract.[155] In the instant case the plaintiff lived as a farmer in Austria with his family. His dwelling place included a pigsty, fodder

150 See Monye *Consumer protection* 15.
151 *Benincasa v Dentalkit* Case C-269/95 (1997) ECR 1-03767.
152 Convention on Jurisdiction and the Enforcement of Judgements in Civil and Commercial Matters 1968.
153 *Benincasa v Dentalkit* supra at 1-03768; see also Tang *Electronic Consumer Contracts* 22.
154 *Gruber v BayWa AG* Case C-464/01 (2005) ECR 1-439.
155 *Gruber v BayWa AG* Case C-464/01 (2005) ECR para 17.

room, fodder silos and machinery room.[156] He approached BayWa AG who had his business location in Germany to tile his farmhouse roof. He introduced himself but he did not specify that he was a farmer.[157] When the contract was concluded the plaintiff was dissatisfied with the colour variations and instituted proceedings against BayWa.[158]

The Court submitted that in determining a mixed contract the predominant ingredient of the entire transaction must be considered and where there is doubt, it should be decided as a consumer contract so as to protect the consumer.[159] In this case however, the Court found that the contract was not a consumer contract.[160] The reasoning could be linked to the use of the farmhouse which though used as a dwelling but most importantly served as a farmhouse. From this perspective, it is immaterial that the contract was not a direct subject of one's trade – such as a woodcutter buying wood to chop – but includes the purchase of any other material or service that would assist in carrying out the trade or profession of chopping wood – for example, buying a packet of pens to record transactions associated with the sale of the wood.[161] However, where the use of the product or service which is put into the trade is negligible – such as the woodcutter buying a pen to record his sales – it is submitted that the buyer will be able to rely on consumer protection.[162]

It appears to be therefore pertinent for merchants to know the status of their buyers. To determine this, consideration should be given to the contract itself, the quantity of goods ordered, and, very importantly, information given by buyers.[163] Currently, certain websites require that buyers specify whether they are acting personally or on behalf of

156 *Gruber v BayWa AG* Case C-464/01 (2005) ECR para 8.
157 *Gruber v BayWa AG* Case C-464/01 (2005) ECR para 10.
158 *Gruber v BayWa AG* Case C-464/01 (2005) ECR para 13.
159 *Gruber v BayWa AG* Case C-464/01 (2005) ECR para 30.
160 *Gruber v BayWa AG* Case C-464/01 (2005) ECR para 52.
161 *Gruber v BayWa AG* Case C-464/01 (2005) ECR para 41.
162 See Judgement of the Court (Second Chamber) 20 January 2005 Johann Gruber v BayWa AG Case C-464/01 para 54.
163 Tang *Electronic Consumer Contracts* 25.

a business.[164] Replies to such enquiries settle the issue of determining the status of the buyer at the point of purchase, although this statement will not protect the buyer where it is established that, contrary to the earlier statement, the contract for goods or services was used for business and not for personal or family use.[165] By and large, it is safer for businesses to assume that every buyer is a consumer until a contrary intention is shown.

2.7.2 Rights of an electronic commerce consumer

In essence, consumers are entitled to rights which safeguard their interests. These rights are available to all, and from them other rights flow.[166] Article 8 of the Universal Declaration of Human Rights (UDHR),[167] provides for the right of every person to redress. This right is reinforced by the consumer's right to effective remedy or compensation, especially through ADR or ODR. Article 10 of the UDHR proclaims the right to fair hearing thus laying the foundation for the protection of consumers against unfair terms in consumer contracts where most terms are skewed and have the effect of excluding the consumer. The protection of consumers from undue interference through spam and direct commercial communication by suppliers is again outlawed in article 12 of the UDHR which preserves the privacy of individuals.

In response to recent developments as a result of the advent of the digital age, the UN Human Rights Council revised its Draft Resolution on the Promotion, Protection and Enjoyment of Human Rights on the Internet.[168] The aims of the resolution include

---

164 See for instance when purchasing potato chips from fritolay.com, you are directed to buy online from Fresh direct which requires that you open an account showing whether delivery is to your home, school or business, available at https://www.freshdirect.com (date of use: 10 October 2020).

165 See the earlier case of *Benincasa v Dentalkit* Case C-269/95 (1997) ECR 1-3767.

166 The Universal Declaration of Human Rights embodies the basic norms of fundamental human rights as proclaimed by the UN in Paris 10 December 1948 as a common standard for all people; closely connected is the International Covenant on Economic, Social and Cultural Rights of 1966.

167 Universal Declaration of Human Rights proclaimed by the United Nations General Assembly in Paris on 10 December 1948 (General Assembly res 217A).

168 General Assembly res 70/1 of June 2016 of the Human Rights Council res A/HRC/32/L.20 on

ensuring that the rights people have offline are also protected online through any medium of one's choice, in accordance with article 19 of both the UDHR and the International Covenant on Civil and Political Rights (ICCPR).[169] The resolution further aims at bridging digital divide, gender digital divide, protecting privacy and other forms of human rights online, and condemns intentional measures to disrupt access to or dissemination of information online as well as other abuses.[170] In Africa especially, the digital divide stems partly from poor education. This constitutes a breach of the right to good education as contained in the International Covenant on Economic, Social and Cultural Rights.[171] The UN resolution on Right to Internet Access accordingly calls on "states to promote digital literacy and facilitate access to information on the internet."[172]

Basic consumer rights have been identified in the different international, regional, and national instruments on consumer protection which have been selected for the purpose of this study. They include the right to information and disclosure, responsible marketing, safety, choice, a fair hearing, reasonable terms and conditions, privacy, withdrawal, redress, and enforcement.[173] The protection of e-commerce consumers through safeguarding these rights will place them on par with other consumers who indulge in conventional commercial practice or face-to-face commercial trade.

---

the Promotion, Protection and Enjoyment of Human Rights on the Internet (Right to Internet Access).

169 International Covenant on Civil and Political Rights adopted by the UN General Assembly res 2200A (XX1) on 16 December 1966, came into force 23 March 1976.

170 Right to Internet Access paras 6, 8 & 10.

171 International Covenant on Economic, Social and Cultural Rights adopted by the UN General Assembly 16 December (1966), came into force 3 January 1976.

172 Right to Internet Access para 4. In response to this call, Nigeria currently has a Bill on Digital Rights and Freedom which the President refused to sign into law (HB 490) Pulse "President Buhari has rejected a bill seeking to protect the rights of internet users in Nigeria from infringement" 21 March 2019 available at https://www.pulse,ng (date of use: 2 July 2020).

173 Each of these rights is considered in subsequent chapters to the extent that they are covered under the enabling laws.

2.7.3 Consumer protection and related concepts

In order to appreciate the study of e-commerce consumer protection law holistically, it is important to understand some of the basic concepts that generate issues under the topic. These concepts are discussed below.

2.7.3.1 Information society services

Most commercial activities on the internet qualify as information society services. These information system or society services include both the sale of products and the delivery of services.[174] The term "information society service" as defined in the E-commerce Directive refers to services

> normally provided for remuneration, at a distance, by means of electronic equipment for the processing (including digital compression) and storage of data, and at the individual request of a recipient of the service.[175]

In terms of the E-commerce Directive, they do not apply to individual communications using e-mail or equivalent means of personal e-communication for the conclusion of contracts.[176] Information society services, therefore, do not cover e-mail contracts between consumers within the EU.

In the SADC Model Law on e-transactions,[177] "information system services" is defined as

> providing the connection and network facilities necessary for transmitting, hosting, and routing electronic communications between or among points of the user's choice specified by a data user, without modification to the content of the data sent, stored, or received.[178]

Information society services do not only apply to the sale of goods online, but also to economic or commercial "services which are not remunerated by those

174 Lodder and Kasperson *e-Directives* 2.
175 E-commerce Directive para 17 of the Recital.
176 Ibid at para 18 of the Recital.
177 SADC Model Law on Electronic Transactions and Electronic Communications, 2012.
178 SADC Model Law s 1(15).

who receive them – for example, offering on-line information or commercial communications, or providing tools allowing for search, access, and retrieval of data..."[179]

This definition of information system services raises four points. First, it introduces the element of distance; second, it links the transaction to remuneration, whether directly or not, provided it is a commercial activity; third, the service must be provided "by means of electronic equipment for processing";[180] and fourth, the service must be provided "at the request of the recipient of the service".[181] Before further discussions, it should be noted that the term used to describe the function of the information society is "service." Service relates to "on-line activities such as the provision of on-line information, on-line advertising, on-line shopping and on-line contracting".[182] Services in this context also include the sale of goods online[183] and Value-added Network Services (VANS).[184]

2.7.3.2 Internet role-players or intermediaries

Network providers consist of international voice/data carriers, service providers, or system integrators which "make information system services available".[185] The roles and liabilities of service providers are discussed below.

(a) Service provider

A service provider is a natural or juristic person who provides services to other persons or entities[186] – in the present context, a natural or legal person providing an information society service.[187] Service providers are not liable for the information they transmit or store, provided that they: do not "initiate the transmission; …select the

179 E-commerce Directive para 18 of the Recital.
180 Ibid.
181 Ibid; see also, UK E-commerce Regulations.
182 E-commerce Directive para 21 of the Recital.
183 E-commerce Directive para 18 of the Recital.
184 Aldaheff and Cohen "Functionality of value-added network providers and their liability" 240.
185 See s 1(20) of the SADC Model Law.
186 Nigerian E-transactions Bill 2017 s 45.
187 E-commerce Directive art 2.

receiver of the transmission; …select or modify the information contained in the transmission."[188] The service provider must not also know or condone information that constitutes an illegal activity.[189]

Service providers are well protected by law so that there are no obstacles to the free flow of information. The law exempts service providers from a general obligation to monitor the services they provide as such an obligation may prove overly restrictive and cumbersome.[190] However, service providers are liable for direct infringement of the law. In 2019, the European Union fined Google €1.49 billion for abusing its market dominance.[191] E-commerce is widespread and easily accessible due to the activities of service providers. Web pages on the internet are estimated to total 5.41 billion pages,[192] while there are an estimated 4.9 billion internet users in the world.[193] These sites are, in the main, commercial and offer all types of opportunities to consumers.

The success of the internet is based largely on the free flow of information and this could be hampered by strict liability or restrictions on service providers.[194] The cost of shopping online could also escalate if service providers were to be weighed down by extreme legal requirements involving the monitoring of sales, payments, and promotions on their sites, and also if they were compelled to take responsibility for fraudulent activities by aggregators on their websites.[195] Data censorship also slows internet traffic[196] and suppliers may inadvertently be discouraged from running online shops in the face of legal challenges, thereby discouraging online sales and

188 E-commerce Directive art 12 (1) a-c.
189 Ibid at art 14; see further, Framework for Cyberlaws Phase 1 2008 R 11.
190 E-commerce Directive art 15.
191 EU "Antitrust: Commission fines Google €1.49 billion for abusive practices in online advertising" 20 March 2019 available at https://www.ec.europa.eu (date of use: 25 November 2020).
192 Worldwidewebsize "The size of the World Wide Web (the internet)", statistics provided as of 16 December 2020 available at www.worldwidewebsize.com (date of use: 20 December 2020).
193 As of 30 September 2020, internet users were estimated at 4, 929, 926, 187 available at www.internetworldstats.com (date of use: 27 November 2020).
194 Esselaar "What ISPs can do" 4.
195 Carnegie Mellon School of Computer Science "The ISPs Role of Improving Internet Security" 27 available at www.cs.cmu.edu (date of use: 22 September 2020).
196 Esselaar "What ISPs can do" 14.

consumer access to a variety of products.[197] Service providers include internet service providers, application service providers, and wireless application service providers.

(i) Internet service providers

Information society services are carried out by ISPs also called online service providers (OSPs). They have the capacity to perform a wide range of activities, the extent of which, however, determines their level of liability online. The services they provide include internet access services, hosting services, website design, transmission of information, and the provision of information-location tools.[198] Certain ISPs provide only internet access, also known as internet access services; some include hosting services; while yet others perform additional internet services such as the transmission of information.

Emphasis is placed on determining the exact role of an ISP in order to establish its level of liability. According to Buys,

> an ISP which provides hosting services, access to the internet, news services on its homepage, and a search engine, plays the roles of access provider, host, content provider, and navigation provider.[199]

In *Goddard v Google Inc*[200] the plaintiff (Goddard), claimed that she and some other persons were harmed when she opened an advertisement on a web page on Google's web site which she later discovered was fraudulent.[201] Google's defence was based on section 230 of the Communications Decency Act (the CDA)[202] "which protects the owner of a website from bearing liability as publisher or speaker of third party content."[203] The court based its findings on the protection available in the CDA and

197 Bernstein and Ramchandani *Canadian Journal of Law & Technology* (2002) 77.
198 E-commerce Directive para 18; Buys "The internet: An overview" 20.
199 Buys and Rothmann "Internet Law and Regulation" 19.
200 *Goddard v Google Inc* 640 F Supp 2d 1193 (ND Cal Jul 30 2009).
201 Ibid at 1195.
202 Computer Decency Act 1996 47 USC S230 (c)(1).
203 *Goddard* 640 F 2d 1195.

held that "…section 230 must be interpreted to protect websites not merely from ultimate liability, but from having to fight costly and protracted legal battles."[204] The court also relied on the case of *Carafano v Metrosplash.com*[205] amongst others and re-stated that "a website operator is not liable as an 'information content provider' merely for augmenting the content of online material generally".[206] Consumers could, however, claim in contract against ISPs when their conduct creates a legal duty outside that of a publisher.[207]

Liability will also arise where an ISP acts as a content provider in addition to hosting, or where the ISP acts as an editor of the content on a site or performs other overt actions. In the case of *Fair Housing Council of San Fernando Valley v Roommates.com, LLC*[208] the court surmised that ISPs are granted immunity where online contents on their websites are created by third parties in line with section 230 of the CDA.[209] The court concluded: "However, information content providers who are responsible, in whole or in part, for the creation or development of infringing materials are not immune."[210]

In the *Roommates.com* case, the court found the ISP (defendant) liable for infringements arising from its discriminatory questionnaires that users were required to complete before they could use the site.[211] In all, internet navigation providers, providers of information-location tools, search engines, or hyperlinks will only be held liable on the basis of the level of control exerted by the provider in respect of the content to which the tool directs the user.[212]

---

204 *Goddard* 640 F 2d 1202.
205 *Carafano v Metrosplash.com* 339 F 3d 1119 (9th Cir 2003).
206 *Goddard* 640 F 2d 1196.
207 *Goddard* 640 F 2d 1200; see the case of *Barnes v Yahoo! Inc* No 05-36189 (9th Cir Jun 22, 2009).
208 *Fair Housing Council of San Fernando Valley v Roommates.com LLC* 521 F 3d 1157 (9th Cir 2008).
209 Ibid *Fair Housing Council of San Fernando Valley v Roommates.com LLC* 521 F 3d 1163.
210 Ibid.
211 *Fair Housing Council of San Fernando Valley v Roommates.com LLC* 521 F 3d 1166-1168.
212 E-commerce directive para 44.

Furthermore, actual knowledge of illicit activities or content to which a provider's tool directs users, could render a provider liable. In order to establish a provider's knowledge, the link or search engine must lead the user directly to the incriminating website and not direct him or her to it through another navigation process. To avoid liability, a service provider who learns of an illegal activity on its website, has a duty to take or block out such information or activity without delay.[213]

In *Sega Enterprises Ltd v MAPHIA*[214] the Northern District Court of California, in the US, had to consider "whether a Bulletin Board Service (BBS) operator was liable for copyright infringement where it solicited subscribers to upload files containing copyrighted materials to the BBS that was available for others to download".[215] The plaintiffs traded in the "manufacture and distribution of computer game systems" and showed in evidence that their video games which were subject to copyright were available on the BB.[216] The plaintiffs further showed that the downloading of their games led to decreased sales.[217] The Court found "a *prima facia* case of direct and contributory infringement by Defendants…" [218] and entered "an order confirming seizure and preliminary injunction."[219]

Access providers could also be liable for fraud through online sales and advertisements, depending on the role they play. Generally, however, there is a limitation on the liability of access providers as it would be unreasonable to hold every service provider liable for acts committed by third parties with whom the provider has an internet access agreement. The summary of the court's finding in *Religious Technology Centre v Netcom On-line Comm*[220] is reproduced below.

---

213 Ibid at para 46. Actual knowledge of illegal activities on the website could be determined through notices and take-down procedures which may earlier have been served on a service provider see Sprindler, Riccio and Van der Perre *Liability of Internet Intermediaries* 14.

214 *Sega Enterprises Ltd v MAPHIA* 857 F Supp 679, 683 (ND Cal 1994).

215 *Sega Enterprises Ltd v MAPHIA* 857 F Supp I683.

216 *Sega Enterprises Ltd v MAPHIA* 857 F Supp 683.

217 *Sega Enterprises Ltd v MAPHIA* 857 F Supp 684.

218 *Sega Enterprises Ltd v MAPHIA* 857 F Supp 687.

219 *Sega Enterprises Ltd v MAPHIA* 857 F Supp 690.

220 *Religious Technology Centre v Netcom On-line Comm* 907 F Supp 1361-Dist Court (ND Cal 1995) para 1f.

> Although the internet consists of many different computers networked together, some of which may contain infringing files, it does not make sense to hold the operator of each computer liable as an infringer merely because his or her computer is linked to a computer with an infringing file. It would be especially inappropriate to hold liable a service that acts more like a conduit, in other words, one that does not itself keep an archive of files for more than a short duration. Finding such a service liable would involve an unreasonably broad construction of public distribution and display rights. No purpose would be served by holding liable those who have no ability to control the information to which their subscribers have access, even though they might be in some sense helping to achieve the internet automatic 'public distribution' and the users' 'public display' of files.

From the reported cases of fraud and misleading advertising by access providers so far considered, and from various cases on copyright infringement, the courts have been consistent on the extent of the liability which can be incurred by an access provider. However, where the access provider is shown to have participated actively in the offending acts in question, it will be held liable. Consumers in such cases could request take-down notices, sue in contract, especially in cases of misleading advertisements, or approach the court for injunctions against the access provider. Nonetheless, it would be advantageous for consumers to determine the role of the ISP in the provision of a service before embarking on litigation or other forms of redress.

(i) Application Service Provider (ASP)

An ASP manages outsourced customer applications[221] which are offered centrally on a lease or on the basis of "pay-as-you-go" over a broadband network to customers who are remotely located.[222] ASPs, more often than not, are managed in partnership with other organisations that have expertise in hardware, software applications, and vertical markets. They offer services which include system integration, e-commerce functionality, customer relations-management, financial packages, and e-mail facilities.[223] Based on their functions, ASPs could be categorised as business service providers (BSPs), or full service providers (FSPs),[224] and further, as network service

221 Rhoton *Wireless Internet Explained* 196.
222 Sparrow *Succesful IT Outsourcing* 228.
223 Ibid.
224 Sparrow *Succesful IT Outsourcing* 229.

providers (NSPs), system integrators (SIs), content service providers (CSPs), independent software vendors (ISVs), value added resellers (VARs), managed security software providers (MSSPs), ASP application aggregators (AAAs), and web developers (WDs).[225]

(ii) Wireless Application Service Provider

A wireless application service provider (WASP) carries out wireless operations.[226] It offers services based on remotely-managed wireless applications to ASP network service providers and directly to customer organisations.[227] WASP is a generic acronym for an industry which provides remote services, especially for handheld devices such as cell phones that connect to wireless data networks.[228] They also engage in modifying existing applications so that the applications can be used by wireless devices for the benefit of software suppliers, integrators, and customers generally.[229]

WASPs could perform either or both services of:

- selling general-purpose wireless applications to other service providers and portals which resell the service to consumers after rebranding;[230]
- developing and leasing specialised applications designed for organisations that wish to offer wireless services to their customers or support mobile staff.[231]

2.7.3.3 Keystroke-error

When conducting business online, it is likely that errors may occur. Errors which occur during the process of inputting data into an electronic system in the course of a

225 Watjatrakul "IT Application Outsourcing: A category and Evaluation of Application Service Pro viders" (2006) 9/4 *Assumption University Journal of Technology* 212.
226 Rhoton *Wireless Internet Explained* 196.
227 Sparrow *Successful IT Outsourcing* 231.
228 Marius "Wireless Application Service Provider" available at https://mybroadband.co.za (date of use: 10 February 2020).
229 Sparrow *Successful IT Outsourcing* 238.
230 Ibid.
231 Ibid.

transaction are keystroke errors or input errors. Consumer transactions can take any of these three forms: “person to person;” “person to e-agent;” or “e-agent to e-agent.” Whatever form it takes, the transaction is protected by law and there are measures for the prevention of errors, and possibly, remedies to situations where the transaction has already been concluded through a keystroke error.

Some laws[232] provide different measures of protection for errors committed by “persons” and errors between a “person and an e-agent.” The EC Convention[233] provides specifically for the prevention of errors between a natural person and an e-agent. It, however, leaves the protection of consumers in the event of other forms of error open to the application of other laws.[234]

It is submitted that protecting the interests of consumers in relation to errors during e-transactions is an essential legislative requirement, for basic consumer protection. Input errors occur frequently, and it could be devastating for the consumer. A consumer could insert an additional digit in a payment transaction or could place double orders by clicking twice in error. Sometimes keystroke errors could lead to a double deduction from the consumer’s account.

In a bid to protect the e-commerce consumer, the EC Convention gives a natural person the right to withdraw from the part of a contract in which the error occurred where an automated message system (AMS) or e-agent does not allow the consumer an opportunity to correct the error.[235] The protection under this provision will, therefore, not avail a consumer who has received a confirmation notice of the transaction generated for his or her consent, and where the consumer proceeded to confirm the transaction without actually correcting any error. While this position can be accepted objectively, the consumer is offered an additional remedy. For instance, a consumer

232 See ss 20 and 43 of the ECTA (South Africa); see also art 14 EC Convention.
233 EC Convention art 14.
234 EC Convention art 14 (2).
235 EC Convention art 14(1); see also s 15(d) Electronic Transactions Act (Australia).

may withdraw from a transaction without providing a reason and without any condition, through the application of a cooling-off period.

Article 6 of the CRD gives effect to the right of withdrawal by providing that without incurring a penalty and without giving reasons, a consumer may withdraw from a contract and will only be responsible for the direct cost of returning the goods where delivery has taken place. In such circumstances, the consumer is entitled to a full refund of the money that has been paid as soon as possible, but within a period not exceeding fourteen days. This right under the Directive can be exercised within fourteen days from the day the goods were delivered, or, in the case of a service, fourteen days from the day of the conclusion of the contract. In cases where the supplier does not comply with the requirement of providing basic information about his or her business before the conclusion of the contract, the period escalates to twelve months.[236] However, if the supplier complies with the information requirement within the twelve-month period, the fourteen-day withdrawal period will begin to run from the day the information was received.[237]

It must be noted that where there are errors and the consumer does not correct the errors or exercise the right to withdraw within the timeframes provided by law, the right will be lost. While there is extensive protection for the consumer, suppliers may only find protection under the common-law principles applicable to voidable contracts due to unilateral mistake by their e-agent.[238]

236 CRD art 10(1).
237 Ibid at art 10(2).
238 Pistorius (2008) 2 *JITL.*

2.7.3.4 Standardised electronic agreements

In the early days of the sale of software, vendors contracted conventionally with each and every end user on an individual basis with the exchange of signatures.[239] The terms of the contract were negotiated by parties to the contract before execution.[240] This ensured that parties were aware of the terms of the transaction, and also had the opportunity to arrange for dispute resolution if necessary. However, following the mass-marketing of computers and the high-volume demand for software, standardised formats are now more convenient as they reduce the cost of negotiating individual contracts, minimize time input and avoid the cost of recurrent litigation in the event of any defect.[241] Most consumer contracts are now based on standard forms.[242] In summary, standardisation saves time and money, and enables software manufacturers to limit liability and warranties.[243] Standard terms lead to contract of adhesion.

Contracts of adhesion are drafted on conditions fixed by one party in advance and are open to acceptance by a purchaser. The contract contains non-negotiable terms and conditions.[244] After establishing that consent is validly obtained, the courts consider the conditions carefully to establish that they are "conscionable" before giving effect to them. These agreements are formed on the basis of unequal bargaining power between the parties. Although inequality of negotiating power is not in itself a ground for invalidating a contract, it must however, be shown that the stronger party took unfair advantage of the position of the other party,[245] as is the case with most software merchants. The courts are wary of contracts based on unequal bargaining power.[246]

---

239 Wang (2015)2 *Journal of Business Law* 93.
240 Gatt (2002) 18 *CLSR* 405.
241 Wilmerhale "The Origin of Click-Wrap: Software Shrink-Wrap Agreements" (2000) available at www.wilmerhale.com (date of use: 14 October 2020).
242 Goodman (2000) 21 *Cardozo L Rev* 319 n 3; Burstein "A Global Network" 31.
243 Evans (2003) 36/1 *Law Theology* 4.
244 Atuos and Walton *French Law* 153.
245 Furmstom *Law of Contract* 21.
246 See the English case of *Schroder Music Publishing Co Ltd v Macauley* (1974) 3 All ER 616 at 624. These forms of electronic agreements, that is, shrink-wrap, click-wrap and web-wrap are discussed further in Chapter 6 with reference to case law.

Standard electronic agreements or contract of adhesion basically include the shrink-wrap, web-wrap or browse-wrap and click-wrap agreements. These agreements are usually contained in the software and can only be accessed after opening or during downloading of the software. The agreements are, in the main, words and are published in very small print, which are sometimes printed on the outside of the software box. In place of the term "shrink-wrap", other terms could also be used by the manufacturers; including "wrap-around", "end-user agreement", "box-top", "tear-me-open", and "blister pack" agreements.[247] These agreements have the mitigating effect of causing undue hardship to consumers sometimes.

2.7.3.5 E-payment system

Payment systems refer to a set of arrangements which is designed for the transfer of value[248] and is executed through various payment platforms including the use of payment cards or electronic money (e-money). EFT is one of the payment systems through which money is transferred electronically to replace one or more of the steps in the process previously served by paper-based systems.[249] The objective of a secured payment system is to limit the risks which consumers may encounter in the course of their transactions online. Consumers may face risks when using credit cards, which could lead to fraud and financial loss should the credit card information be hijacked or misused.[250] However, where there is an unauthorised transaction, the bank bears the liability.[251] The payment system involves the use of merchants,[252] acquirers,[253] issuers,[254] card holders,[255] and e-money.[256] E-money is defined in article 2 of the E-money Directive as

247 Goodman (2000) *Cardozo L Review* 21.
248 Lawack *Electronic Payment Systems* 1.
249 Visser (1989) 1 *SA Merc LJ* 200.
250 Derick "Online Banking Law and Payment Systems" 279 evaluates the main purpose of the Na tional Payment System Act 78 of 1998 in relation to consumer protection.
251 Schulze (2007) 19 *SA Merc LJ* 382.
252 This is the owner of an online store or mall from which purchases are made that accepts payment cards according to an agreement with a merchant bank, see definition in First Data *Payments Industry Glossary* (2012) available at https://firstdata.com. (date of use: 14 October 2020) 9. Some stores operating in real time also accept payment by cards and qualify as merchants.
253 The acquirer is also referred to as the Merchant Bank. It is the financial institution that 'acquires'

> electronically, including magnetically, stored monetary value as represented by a claim on the issuer which is issued on receipt of funds for the purpose of making payment transactions and which is accepted by a natural or legal person other than the electronic money issuer.

E-money, digital purse, and e-wallet are all used synonymously to represent a card with an embedded computer chip which can be "charged" by a bank or any other financial institution.[257]

2.7.3.6 Chargeback

With online sales and purchases, there are situations where consumers are burdened when they receive wrong orders, unauthorised debits for transactions which were not concluded, as well as deductions for products or services which were not delivered. Chargeback has been defined as "the technical term used by international card schemes for the refunding process in respect of a transaction carried out by card following the violation of a rule".[258] The implementation of chargebacks at the domestic level can differ from implementation on the trans-border level. The relative importance of the framework governing chargeback relies on a state's national provision.[259] As the

---

the transaction from the merchant and passes it on to the issuer for payment see European Payment Institutions Federation "Merchant Acquiring" available at https://paymentinstitutions.eu (date of use: 14 October 2020) 1-3; Payments Newsletter "Demystifying the Merchant Acquiring Business" (2018) available at https://www.pwc.in (date of use: 14 October 2020) 2.

254 This is the financial institution that issues a card to a cardholder in terms of an agreement between the two parties (known as a cardholder agreement). An example is the First Bank of Nigeria PLC, for details see "The payments system-overview" available at www.aph.gov.au (date of use: 14 October 2020).

255 The cardholder is the consumer who receives the card from the issuer, First Data *Payments Industry Glossary* 4.

256 Directive 2009/110/EC of the European Parliament and of the Council of 16 September, 2009, on the taking up, pursuit and prudential supervision of the business of electronic money institutions, amending Directives 2005/60/EC and 2006/48/EC and repealing Directive 2000/46/EC (E-money Directive) *Offical Journal* L 267,10.10.2009.

257 Wenninger and Laster (1995) 1/1 *Current Issues in Economics and Finance* 2; Stuber *The elec tronic purse* 3-6.

258 European Commission (European Commission on Chargeback) *Payment Card Chargeback When Paying over the Internet* (2000) 5.

259 European Consumer Centers/Network *Chargeback in the EU/EEA* (A solution to get your mon-ey back when a trader does not respect your consumer rights) 17 available at http://ec.europakonsument.at pdf (date of use: 18 September 2020).

chargeback or cash pay back system is yet to be adopted internationally, the cardholder contract is regulated by national laws.[260]

Chargeback processes are categorised[261] and present problems for banks or card issuers because of the high costs involved.[262] Suffice it to say that some merchants have gone bankrupt because of non-payment for sales performed over the internet.[263] The table below gives chargeback statistics of five countries. It is based on a questionnaire completed by representatives of EU member states as part of the work of the first sub-group (Payment over the internet) established as a working group of the European Commission to study the questions raised by payments online.[264] The five countries are: Germany, France, Italy, Netherlands, and Sweden.

260 European Commission (European Commission on Chargeback) *Payment Card Chargeback When Paying over the Internet* (2000) 6.

261 The processes could be based on lack of card holder authorisation, not receiving purchases or delivery of defective goods - see European Commission (European Commission on Charge-back) *Payment Card Chargeback When Paying over the Internet* (2000) 5.

262 European Commission *Payment Card Chargeback When Paying over the Internet* (2000) 5.

263 Ibid.

264 European Commission (European Commission on Chargeback) *Payment Card Chargeback When Paying over the Internet* (2000) 6.

Table 2.1 Chargeback statistics

COUNTRY	CARD SCHEME	% OF INTERNET-RELATED CHARGE BACKS	% WHICH ARE CROSS-BORDER TRANSACTIONS	'I DID NOT DO IT'	'I DID NOT RECEIVE IT'	'I DO NOT WANT IT'
Germany	Eurocard/Master Card & Visa	**40%-50%**	**80%-90%**	**80%**		
France	Cartes Bancaires	**83%**	**-**	**50%**		
Italy	Eurocard/Master Card & Visa	**58%**	**96.7%**	**99.7%**	**0.10%**	
Netherlands	Eurocard/Master Card	**70%-80%**	**N/A**	**98.32 %**	**1.61%**	**0.07%**
Sweden	Eurocard/Master Card & Visa	**35%-40%**	**99%**	**100%**		

Chargebacks can be applied to protect consumer interest in e-commerce transactions and where applicable, cross-border transactions.

For purposes of re-imbursement in the event of withdrawal, fraud, or abuse of payment systems, Regulation 76 of the UK Payment Services Regulations[265] provides for the legal right to be reimbursed. It provides that, subject to a time limit, in the event

265 The Payment Services Regulations 2017 (UK).

of fraudulent use, consumers are credited with the amounts paid.[266] Furthermore, paragraph vi of the OECD Guidelines on Fraudulent and Deceptive Practices[267] enjoins member countries to address issues pertaining to deceptive practices in e-commerce by providing redress systems for consumers who fall victim to such abuse.[268] Although the EC Convention in its article 14 refers to the right to withdraw from a contract fraught with errors especially in a contract with an AMS, it however, fails to address the effect of such a withdrawal where payment has already been made, or to any formalities aimed at addressing a refund process.

2.7.3.7 Computer cookies

Computer cookies have been defined as

> a string of text data used in information systems to remember a user or visitor to a website, in order to identify appropriate content, and to differentiate between users and maintain data related to the user during the navigation of a website or an information system.[269]

Cookies are small text files which are sent from the server of a web site accessed and saved on the user's hard drive. Through this, there is a track on user information and activity on the website.[270] The use of cookies could lead to a breach of data privacy where the collected information is given or sold to third parties. This information can be used by spammers for direct "phishing".[271] It is also possible to collect credit-card information used on a website through cookies and this could compromise a consumer's payment information. The collection and unauthorised use or

266 Ibid at reg 76.

267 OECD Guidelines for Protecting Consumers from Fraudulent and Deceptive Commercial Practices Across Borders (2003).

268 Ibid.

269 E-transactions Bill art 45.

270 For further reading on cookies, web bugs, and similar technologies see Akhigbe *Legal Framework for Data Protection* 6-7*;* see also Buys and Cronje (eds) *CyberLaw @ SA*-386.

271 Phishing is "the criminal and fraudulent process of attempting to acquire sensitive information such as usernames, passwords and credit card details…" s 58 Cybercrimes (Prohibition, Prevention, etc) Act, 2015.

dissemination of personal data is prohibited and is addressed in various national and regional laws.[272]

Some websites seek the permission of users when using cookies on their websites. This enables consumers to decline their use or disable cookies through their web browsers.

2.7.3.8 Spam

Spam constitutes unsolicited or inappropriate messages or commercial communications which are sent to a large number of recipients without their consent thus posing challenges to consumers' privacy in the electronic marketplace.[273] The dangers in spam range from messages targeted at collecting personal data such as bank details in order to perpetuate fraud, denial-of-service attack, identity theft, or malware in a system. It is, of course, also a time-consuming irritation and nuisance to the recipient; with run-off consequences like additional cost on consumers and unnecessary consumption of storage space.[274] Spam could be perpetuated by a "botherder"[275] through the use of a botnet on the internet.

---

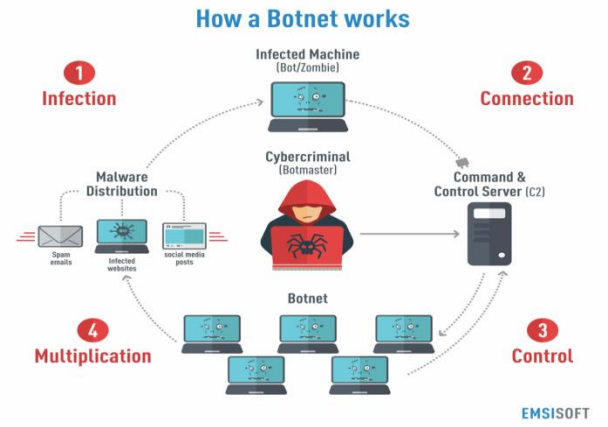
272 See, for example, the following: AU Convention on Cyber Security and Personal Data Protection, 2012; General Data Protection Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016; Organisation for Economic Cooperation and Development (OECD) Guidelines on the Protection of Individuals with Regard to the Processing of Personal Data, 1981; Federal Privacy Act, 1988 (Australia); Nigeria E-transactions Bill, 2017; Protection of Personal Information Act 4 of 2013 (South Africa); Electronic Communications Privacy Act Amendment Act of 2015 amending the Electronic Communications Privacy Act, 1986 (18 United States Congress); and the Data Protection Act, 2018 (UK).

273 Tladi (2008) 125/1 *The South African Law Journal* 179*;* Akhigbe (2019) *6 Benin Journal of Public Law* 195-196.

274 Tladi (2008) 125/1 *The South African Law Journal* 183; Army (2005) 33/4 *Pepperdine Law Review* 1041.

275 A botherder is defined as an individual or hacker 'who controls and maintains a botnet by installing malicious software on numerous machines. These "herds" of bot machines, also called zombies, are then used to attack or infect other machines' see Techopedia "What is a botnet herder?" available at www.techopedia.com (date of use: 20 September 2020). While a botnet is defined as a number of internet-connected devices infected with malicious software which is used to perform distributed denial of service attack (DDoS), steal data, or send spam, available at http://searchsecurity.techtarget.com (date of use: 20 September 2020).

Diagram 2.2 Effect of Spam



Courtesy: emsisoft available at https://blog.emsisoft.com (date of use: 20 July 2020).

In Europe, particularly EU countries which regulate electronic commerce principally through the EU Directive spam or unsolicited commercial communication is mentioned. Though, the E-commerce Directive did not directly address issues arising from unsolicited commercial communications since it was dealt with in the 1997 Directive on Telecommunications.[276] Based on the Directive on Telecommunications the E-commerce Directive in its article seven provides that where commercial communications are permitted they must be clearly identifiable and should provide easy opt out approaches. In this way, consumers are given the opportunity clearly to identify spam messages and eliminate them.[277] The elaborate legislation on spam in some countries notwithstanding, spamming has continued to be a scourge to consumers globally. Trying to trace and prosecute spammers outside the consumers' jurisdiction is always a problem.[278] In order to eliminate the problem of spam tactically,

276 See E-commerce Directive Preamble para 30 and art 7; see also Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 Concerning the Processing of Personal Data and the Protection of Privacy in the Telecommunications Sector (Directive on Telecommunications). This Directive has been repealed by Directive 2002/58/EC of the European Parliament and of the Council 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).

277 Kuner "Directive 2000/31/EC-Directive on Electronic Commerce" 237-238.

278 Hamann and Papadopoulous (2014) *De Jure* 50.

the EU came up with a Directive on Privacy and Electronic Communications.[279] Article 7(2) of the E-commerce Directive applies to natural persons and is interpreted in line with the Privacy and Electronic Communications Directive. The Directive on Privacy and Electronic Communication, does not allow the dissemination of unsolicited commercial e-mails unless prior consent has been given by the recipient.[280] Suppliers may, however, contact recipients using details which were earlier obtained during sale or services, to market similar products in so far, recipients are able to object freely and easily, should they so wish.[281]

2.7.3.9 Automated transaction

Data messages can be automated by using "an information system that is programmed by, or on behalf of, the originator to operate automatically."[282] Messages using such a process are legally recognised, valid, and enforceable,[283] and give rise to automated transactions.

> An automated transaction is a transaction that could be conducted or performed, in whole or in part, by electronic means or electronic records, in which the acts or records of one or both parties are not reviewed by an individual in the ordinary course in forming a contract, performing under an existing contract, or fulfilling an obligation required by the transaction.[284]

279 Directive 2002/58/EC on Privacy and Electronic Communications. This Directive will be repealed by the ePrivacy Regulation once it comes into effect. The ePrivacy Regulation and the GDRP were scheduled to come into effect on the 25 May 2018. However, following some amendments the ePrivacy Regulation was not implemented and may not be implemented until 2021, see Lexology "EU updates: ePrivacy Regulations inches forward, EDPB issues guidance on interplay between GDPR and ePrivacy Directive" available at https://www.lexology.com (date of use: 25 November 2019).

280 Privacy and Electronic Communications Directive see art 10(4) & 13. Spam makes communication cumbersome and leads to loss of time and lingering cost of data for consumers. On the effect of spam on consumers see Schryen *Anti-spam measures* 22; Grossman (2014) 19/4 *Berkeley Technology Law Journal* 1544.

281 Privacy and Electronic Communications Directive art 13(1)(4). It should be noted that article 6(f) of the GDRP permits processing of a consumer's information in the absence of his or her consent when the processing is for a legitimate purpose. This could apply to a supplier who contacts his or her existing customer for marketing purposes.

282 See art 13 (2)(b) UNCITRAL Model Law.

283 See art 5 UNCITRAL Model Law; art 12 EC Convention.

284 US Uniform Electronics Transactions Act s 322 (2).

An automated transaction is legally binding on the contracting parties provided that the transaction was formed through a regular course or procedure previously known or agreed to by the parties; or through the action of a person or agent related to the originator of the automated system, through which the originator can identify the automated system as its own. An automated transaction may be unenforceable under certain conditions.[285] Electronic systems that perform automated transactions are usually referred to as an Automated Message System (AMS)[286] or as e-agent, software-agent, mobile-agent, electronic robot, or shopping agent.

2.7.3.10 Electronic agents

E-agents are "computer programmes or other electronic or automated means configured and enabled by a person, that are used to initiate or respond to electronic records or performance, in whole or in part, without being reviewed by an individual".[287] E-agents are "able to perform inter-systemic electronic contracting functions."[288] They are autonomous,[289] socially interactive,[290] responsive,[291] and proactive.[292]

The e-agent could be located in an e-shopping mall, on the consumer's computer, or on an external server managed by a provider. The location of the e-agent influences its output. An e-agent located in a shopping mall tends to deliver quick search results since it is located within the mall. It is however, restricted to its specific location and is, therefore, incapable of providing comparative prices from other malls.[293]

---

285 The conditions would include where: there is adequate notice to a recipient denying a data message, art 13(4) UNCITRAL Model Law; there is an input error without means of correcting the error, art 14 EC Convention; where a consumer exercises the right of withdrawal within statutory time, EC Convention art 4(g).

286 EC Convention on Electronic Communications art 4(g).

287 The Electronic Transactions Bill art 45; US Uniform Electronic Transactions Act s 322(2).

288 Andrade, Novais and Neves "Will and Declaration" 2.

289 Casterfranchi "Guarantees for autonomy in cognitive Agent Architecture" 56-70.

290 Wooldridge and Jennings "Applications of Intelligent Agents" 3-5.

291 Ibid.

292 Haentjens "Shopping Agents and their Legal implications regarding Austrian Law" (2011) available at www.citeseerx.ist.psu.edu (date of use: 28 June 2020) 2.

293 Beykirch and Handeln (1998) ix *Magazin fur professionelle Informationstechnik* S 122f, 3.

This is unlike the e-agent which is located in an external server and which is capable of conducting widespread searches. Such an e-agent can produce a comprehensive product-range as it is not restricted to a specific shopping mall or location. Again, the e-agent is able to work round the clock as the attention of the principal is not required, and it can be accessed from any other computer in addition to that of the consumer or principal.[294]

These advantages notwithstanding, there is considerable danger in relying on the application of e-agents both for the merchant and for the consumer as there can be errors.[295] Wrong or conflicting commands can mistakenly be fed into the system; hardware failure can alter how the system functions; while viruses and physical interference can cause the system to malfunction. In any of these cases, an e-agent could continue to process and conclude orders for sale – especially during promotional offers – where in actual fact the store has run out of stock. The output of the e-agent may also be restricted as some merchants block the use of e-agents on their sites in order to protect their businesses.[296] Some sites also block e-agents in an attempt to promote visits by humans. This may boost their income through advertising on their sites which is visible only to humans.[297]

Another challenge arises where the agent has to pay for a service, or be paid for a service, in its usual schedule. This task demands a high level of security and fault resistance to ensure that the order is not lost or duplicated.[298] The greatest challenge facing the consumer occurs where, in the process of concluding a contract, the e-agent has to agree to the terms and conditions of the supplier or his or her sales

294 Pomp "Konzept und Implementierung eines Shopping-Agenten-Systems fur elektronische Marktplatze" 2 available at http://www.medienassistent.org (date of use: 16 September 2020).
295 Leng (2006) 22 *Computer Law & Security Report* 158.
296 Leng (2006) 22 *Computer Law & Security Report* 158; Ismail and Kamat (2006) 132 *Journal of Professional Issues in Engineering Education and Practice* 356-357.
297 Kotz & Gray "Mobile Agents and the Future of the Internet" available at http://www.cs.dartmouth.edu (date of use: 21 August 2020).
298 Vogler, Moschgath and Kunkelmann"Enhancing Mobile Agents" 149.

agent. The consumer would of necessity need to programme its agent in such a way that it only goes into agreement with sites which provide acceptable contract terms.[299]

While achieving this is doubtful, there are proposals for the use of Extensible Markup Language (XML) for computers, as opposed to the format-oriented, handcrafted, HTML which can be perceived only by the human eye.[300] It has also been proposed that e-agents should be guided on a line-up of contractual terms which it can accept.[301] It is submitted that the flaw in this proposal is that it is impractical due to the ever changing and evolving demands of suppliers across different business environments.

Legally, the wrongful use of e-agents could incur liability for the user or principal. In *Registrar.Com Inc v Verio Inc*,[302] the court held that the use of a robot to gather information on a website which outlawed the use of robots amounted to "trespass to chattels." [303] The court further found the defendant liable for damages to the computer system under section (a)(5)(A-C) of the Computer Fraud and Abuse Act [304] as the presence of the robot in the plaintiff's computer was capable of reducing the server's capacity and response time, limiting the availability of data to clients, and could even cause the plaintiff's computer to malfunction and crash.[305] From a technological perspective, in order to build trust in the use of e-agents, the strengthening of internal and external security, as well as data security has been proposed.[306]

---

299 Haentjens O "Shopping Agents and their Legal implications regarding Austrian Law" (2011) available at www.citeseerx.ist.psu.edu (date of use: 28 June 2020) 8.

300 See further, Reagle, Eskimo and Scottish *Considerations of Schema Design (*1999) Berkman Centre Working Draft https://cyber.harvard.edu le 1999 1-27 available at www.w3.org/tr/1999/note (date of use: 28 June 2019); and Glushko, Tenenbaum & Meltzer (1999) 42/3 *Communications of the ACM* 107.

301 Pomp (MMS) "Konzept und Implementierung eines Shopping-Agenten-Systems fur elektronische Marktplatze" 2 available at http://www.medienassistent.org (date of use: 16 September 2020).

302 *Registrar.Com Inc v Verio Inc* 126 F Supp 2d 238 Dist Court (SD New York 2000).

303 Ibid at 250.

304 Ibid at 252-253; see also Computer Fraud and Abuse Act (1986) 18 USC s1030 as amended.

305 *Registrar.Com Inc* 126 F 2d at 251.

306 See Calmet and Endsuleit "An Agent Framework for Legal Validation of E-Transaction" (2004) Allien Institute for Artificial Intelligence 182-3.

The next area of importance is a consideration of the legal classification of e-agents and the enforceability of the contracts they conclude. An e-agent acts on behalf of the user but does not qualify as a "person" with legal personality in that it is simply a "system or programme." Article 2 of the UNCITRAL Model Law[307] gives two distinct definitions for the management of data. It defines an intermediary as a "person who sends, receives, or stores data messages, or provides other services with respect to that data message on behalf of another person." On the other hand, it defines an information system as a "system for generating, sending, receiving, storing, or otherwise processing, data messages." Paragraph 35 of the Guide to the UNCITRAL Model Law provides that "the law should not be misinterpreted as allowing for a computer to be the subject of rights and obligations"; it should not have legal personality.

It is submitted that the validity of automated transactions should derive from the users of the system. The e-agent acts on the authority of the user, who in this case is the principal, and the substantive law of agency apply between the user or originator and the e-agent. Therefore, contracts formed by interaction between e-agents, or an e-agent and a natural person, with or without any review by a natural person(s), are valid provided that other substantive requirements for validity[308] have been met, and are, therefore, enforceable against the parties. Article 12 of the EC Convention provides:

> A contract formed by the interaction of an automated message system and a natural person, or by the interaction of automated messages, shall not be denied validity or enforceability on the sole ground that no natural person reviewed or intervened in each of the individual actions carried out by the automated message systems or the resulting contract.

307 The UNCITRAL Model Law is discussed in more details in Chapter 3 of this study.

308 Generally, all contracts whether offline or online, are subject to the general laws of validation of contracts which include capacity; intent; consideration, and legality.

2.7.3.11 Electronic transferable record

A "transferable record" is a general term that refers both to a transferable instrument as well as to a transferable document of title. An electronic transferable record is the electronic equivalent of a transferable record.

> Transferable instruments are financial instruments that may contain either an unconditional promise to pay a fixed amount of money to the holder of the instrument, or an order to a third party to pay the holder of the instrument.[309]

Examples of transferable instruments include "promissory notes, bills of exchange, cheques, and certificates of deposit."[310]

The use of e-transferable documents is to create functional electronic equivalence in the use of transferable documents. Its use is also to eliminate barriers in the area of documents of transfer in e-commerce.[311]

2.7.3.12 Jurisdiction

Jurisdiction is fundamental to the resolution of any dispute whether criminal, commercial or in the application of rights. Courts must be granted the powers to adjudicate over issues arising from the presence of the parties within the territory of the court; over property within the jurisdiction or in respect of certain subject matters.[312] The general rules on jurisdiction are guided by factors such as the conclusion of the contract within a jurisdiction,[313] the defendant's submission to jurisdiction, the defendant owning a landed property within jurisdiction,[314] or a breach of contract within jurisdiction.[315]

---

309 UNCITRAL Working Group iv (Electronic Commerce) 46th Session 2012 "Legal Issues Relating to the Use of Electronic Transferable Records" 3.

310 Ibid.

311 Alba (2013) 5 *Creighton International and Comparative Law Journal* 2.

312 Amro (2016) 20 *Vindobona Journal of International Commercial Law & Arbitration* 9.

313 McNamara & O'Shea "Minimising legal risks in electronic contracting" 5.

314 Cameron (2001) 34 *Law/Technology* 3.

315 Although where a breach of contract takes place is not universally accepted as a ground for establishing jurisdiction, see Forsyth *Private International Law* 215.

In determining jurisdiction involving a foreign defendant, connecting factors become important and they are based either on the domicile of a party or on the location of the business.[316] But in internet cases, there is no physical presence and business presence cannot be linked to the location of a server or other equipment. The connecting factor, therefore, can only be established on the basis of the nature of the activities of a website owner in a particular forum. Where these activities are active or intermediate, then there is a connecting factor to the jurisdiction where such a website pursues its economic activities.[317]

The borderless and anonymous nature of the internet, negate all the principles governing the rules of courts in assuming jurisdiction over disputes regarding online transactions. This stance has been and remains a work area in internet law as the legal activity of service providers in one jurisdiction may be illegal in another jurisdiction.[318]

Meanwhile a resolution of the challenges raised in cross border jurisdiction is proposed by the Hague Conference. The Hague Conference is an intergovernmental organisation working to unify private international law rules. Its first session was held in 1893 and after seven further sessions, a statute came into operation in 1955 establishing the Conference as a permanent organisation. The Conference has 83 members. The membership is made up of 82 states and one Regional Integration Organisation. They hold plenary sessions to discuss and adopt draft conventions and recommendations, and to take decisions on their working agenda.[319] The principal role of the Conference is to negotiate and draft multinational treaties or conventions in the different areas of private international law. Its areas of concern include: conflict of jurisdictions; applicable law; and international judicial and administrative cooperation

316 Dicey, Morris & Collins *The Conflict of Laws* 100.

317 See the cases of *Clipp Designs v Tag Bags* 1996 F Supp 766 (ND 111 1998); *International Shoe Co v Washington* 326 US 310 (SC of US 1945) and the discussion in chap 6 para 6.7.1

318 Kightlinger (2003) 24/3 *Michigan Journal of International Law* 720; Goldring J (1996) 2/2 *Journal of Computer Mediated Communication* 4.

319 HCCH "Members and parties" available at https://www.hcch.net (date of use: 20 October 2020).

regarding civil liability for environmental damage; problems of private international law raised by electronic interchange; and maintenance obligations.[320]

The Hague Conference aims to offer a harmonised rule establishing the applicable jurisdiction in international contracts, as an addition to the role played by the 1971 Convention on the Recognition and Enforcement of Foreign Judgments in Civil and Commercial Matters. In 1999, the Hague Conference on Private International Law held a round table discussion (in conjunction with the University of Geneva) involving experts in various fields, on issues arising from e-commerce and internet transactions. A series of recommendations were adopted in areas such as: online contracts; B2B and B2C transactions; and online dispute resolution. [321] At the meeting the recommendations of the roundtable were that e-commerce did not require new norms, rather old norms should be adapted to suit e-commerce by the use of functional equivalents. The round table further recommended that when new norms were created they should be technology neutral. Applicable law and jurisdiction in online contracts which were performed offline should follow existing private international rules on place of performance. Where however, performance takes place offline, the connecting factor should be the location of each of the contractual parties. Further recommendations were however, to be considered in b2c transactions with emphasis on the adoption of the proposed HCCH Convention on Jurisdiction and Judgement.[322] It should be noted however, that on 2nd July 2019 the 222nd Diplomatic Session of the HCCH signed and adopted the 2019 Convention on the Recognition and Enforcement of Foreign Judgements in Civil or Commercial Matters.[323]

320 HCCH "More about HCCH" available at https://www.hcchh.net/en/home (date of use: 09 October 2020).

321 HCCH "Electronic commerce and the internet" (Press release 26 June 2003) the meeting took place on 2,3, & 4 September 1999 and was attended by 100 experts representing 26 countries and fourteen international governmental and non-governmental organisations, available at https://www.hcch.net (date of use: 20 October 2020).

322 Ibid.

323 The Convention was signed at the Hague, Netherlands. Contrary to expectation the Convention does not address jurisdiction. The Convention is not yet in force but has however been signed by some countries, the first country to sign the Convention was Uruguay, available at https://www.hcch.net (date of use: 20 October 2020).

In the course of this study the different approaches employed by different regions will be addressed while currying the path for an international response.

2.8 Summary and conclusion

The creation of the computer and how its connectivity evolved into an internet solution was discussed in this chapter. Distance trade through the use of computers emerged, and this was soon overtaken by e-commerce. There was further discussion on e-commerce, payment concepts, understanding who a consumer is, and issues affecting consumer transactions. Having identified a consumer, the focus of this research in subsequent chapters will be on the legal protection available to consumers who are involved in e-transactions.

In the next chapter, the validity of e-transactions in the international context will be examined relying on the UNCITRAL Model Law and other related instruments of the UN. The UNCITRAL Model Law sets the standard for the functional equivalence of paper-based documents in electronic form. The chapter will address fundamental issues which form the basis of paper records and how these issues are effectively resolved through basic rules on the application of data messages.

CHAPTER THREE

INTERNATIONAL PROTECTION OF E-COMMERCE CONSUMERS: THE UNITED NATIONS

3.1 Introduction

Trends in e-commerce activities have prompted regional and international communities to reflect on the removal of barriers that hinder the free flow of commerce in their communities.[1] Divergent legislation governing the protection of e-commerce consumers provide differing levels of protection for consumers, especially where principles in the different jurisdictions do not provide the same level of protection. Again, not all jurisdictions have consumer protection legislation specific to the electronic environment. This challenge is further heightened by the difficulties of resolving disputes when they arise due to the expense and trouble in seeking cross-border redress and enforcement.

To resolve these issues, various institutions, at both the international and regional levels have enacted regulations and laws on the use of e-communications with the aim of providing certainty and uniformity within their regions. In this chapter, legislative instruments emanating from the UN will be reviewed to assess the measures put in place for the harmonisation of e-commerce principles.

3.1.1 The United Nations

The UN is an international organisation with membership "open to all other peace loving states which accept the obligations contained in the Charter, and which, in the judgement of the organisation, are willing and able to carry these obligations."[2] States are admitted to membership of the UN by a decision of the General Assembly on the

1 Lakhani (2015) *Vindbona Journal of International Law & Arbitration* 82.
2 Article 2 of the UN Charter 26 June 1945. The UN Charter came into force 24 October 1945.

recommendation of the Security Council (SC).[3] It is an international organisation open to all countries, while all other organisations considered in this study, are regional in nature owing either to their geographic spread or economic interest.[4] The UN was established following the conclusion of the Second World War, in the light of allied planning and intentions expressed during that conflict.[5]

The purposes of the UN are to

> maintain international peace and security;… to develop friendly relations among nations based on respect for the principle of equal rights and self-determination of peoples; to achieve international cooperation in resolving international problems of an economic, social, cultural or humanitarian character;… and to be a centre for harmonising the actions of nations in the attainment of these common ends.[6]

Currently, the UN has 220 members[7] and six principal organs: the Security Council SC; the General Assembly (GA); the Economic and Social Council (ESC); the Trusteeship Council; the Secretariat; and the International Court of Justice (ICJ).[8] The GA is the parliamentary body of the UN and consists of representatives of all the member states. To aid its work, the GA has six principal organs, two standing committees, and a number of subsidiary *ad hoc* and other bodies dealing with relevant issues. One of these bodies is the United Nations Commission on International Trade Law (UNCITRAL).[9]

3.1.2 United Nations Commission on International Trade Law

The UNCITRAL is a subsidiary body of the UN, established by the GA

---

3 UN Charter art 4.

4 The UN is open to countries from all over the world; while EU membership is open only to members of the European Community; OECD membership is drawn from 38 countries across different regions see OECD "Where: Global reach" available at www.oecd.org (date of use: 05 September 2020); while membership of other regional organisations is a reflection of their geographic location – e.g, the African Union.

5 UNC 10, 15 Vols, 1945 cited in Shaw *International Law* at 825; see further *History of the UN* available at www.history.com/topics (date of use: 28 August 2020).

6 Article 1 UN Charter.

7 UN "Member states" available at www.un.org (date of use: 25 November 2020).

8 Shaw *International Law* 825.

9 Shaw *International Law* 832.

> with a mandate to further the progressive harmonisation and unification of the law of international trade, and in that regard to bear in mind the interests of all peoples and, in particular, those from developing countries, in the development of international trade.[10]

The body prepares international instruments in respect of commercial transactions.[11] At the 17th session of the Commission in 1984, a report by the UN Secretary-General entitled "Legal Aspects of Automatic Data Processing"[12] was considered. In the report, several legal concerns relating to the legal status of computer records and authentication, among other issues, were identified. The report suggested that as these issues essentially involved international trade law, the UNCITRAL was the best organ of the UN to proffer solutions.[13] In a sequel to the 1983 report, the UNCITRAL made the following recommendations to governments which are para-phrased below:

(a) to review the legal rules affecting the use of computer records as evidence in litigation in order to eliminate unnecessary obstacles to their admission;[14]
(b) to review legal requirements that certain trade transactions or trade related documents be in writing with a view to permitting, where appropriate, the transaction or document to be recorded and transmitted in computer-readable form;[15]
(c) to review legal requirements of a handwritten signature or other paper-based method of authentication;[16]
(d) to review legal requirements that documents for submission to governments are in writing and manually signed.[17]

However, after the 1985 UNCITRAL recommendations,

> there was a general feeling that little progress had been made in achieving the removal of the mandatory requirements from national legislation regarding the use of paper and hand-written signatures.[18]

According to the Norwegian Committee on Trade Procedures (NORPRO), the reason for this feeling could be drawn from the fact that although the 1985 UNCITRAL

10 General Assembly res 2205 (xxi) of 17 December 1996.
11 One of such instruments is the EC Convention, United Nations Publication Sales No E.07.v.2.
12 UN *Legal aspects of automatic data processing: note by the Secretariat* 1983.
13 Magnus *Global Trade Law* 50.
14 Guide to enactment UNCITRAL Model Law para 126.
15 Ibid.
16 Ibid.
17 Ibid. These recommendations were endorsed by GA resolution 40/71 of 11 December 1985.
18 Guide to Enactment UNCITRAL Model Law para 128.

recommendations advocated legal reforms, it however, gave no indication of how those reforms could be achieved.[19]

This perception informed the UNCITRAL's decision to formulate a "model law" for legal issues relating to electronic data interchange and other electronic means of communication. The UNCITRAL Model Law on Electronic Commerce (UNCITRAL Model Law) was subsequently adopted in 1996 with an additional article 5*bis* adopted in 1998.[20] In 2001, the UNCITRAL Model Law on Electronic Signatures was adopted, and in 2005, the UN took a further step to promote e-commerce and ensure protection for recipients of the service by the introduction of the UN Convention on the Use of Electronic Communications in International Contracts (EC Convention).[21]

3.2 The UN Convention on the use of Electronic Communications 2005

The EC Convention was adopted in the belief that the adoption of uniform rules would create a legal environment for e-contracts "acceptable to states with different legal, social, and economic systems".[22] The Convention is binding on states who have domesticated its provision in their national laws.[23]

The EC Convention is technologically neutral and provides electronic equivalence to the use of paper.[24] It has four Chapters: Chapter 1 addresses the scope of application

19 Ibid.

20 General Assembly res 51/162 of 16 December 1996 adopted by the United Nations Commission on International Trade Law (UNCITRAL) Model Law on Electronic Commerce (with additional art 5*bis* adopted in 1998).

21 The EC Convention was adopted on 23 November 2005 at the 53rd plenary session of the GA by resolution A/60/21, and entered into force on 1 March 2013.

22 Recital to the EC Convention.

23 By the very nature of international conventions, they are not binding on states that are not party to them. States become party to a convention by signature or accession. However, accession alone does not implement the convention in the acceding state's national law unless the convention has been incorporated into national law or "domesticated". Currently, eleven countries have domesticated the Convention, see UNCITRAL "Status: United Nations Convention on the Use of Electronic Communications in International Contracts (New York, 2005)" available at www.uncitral.org (date of use: 11 October 2020).

24 Preamble to the EC Convention para 46.

of the Convention and provides for exclusions and party autonomy; Chapter 2 deals with definitions, interpretation, the location of parties, and information requirements; Chapter 3 provides for the use of e-communications in international contracts, including the legal recognition of e-communications, and general requirements for the validity of contracts; while Chapter 4 contains final provisions on ratification, regional participation, and other forms of application.

The EC Convention does not apply to e-communications in respect of "contracts concluded for personal, family, or household purposes"[25] or to "transactions on a regulated exchange."[26]

Furthermore, in terms of article 2, the EC Convention:

> does not apply to bills of exchange, promissory notes, consignment notes, bills of lading, warehouse receipts, or any transferable document or instrument that entitles the bearer or beneficiary to claim the delivery of goods or the payment of a sum of money.

The EC Convention in its article 7 recognises the need for parties to disclose relevant information when doing business. The EC Convention further provides rules on offer, the use of AMS, and a solution for errors arising from the use of AMS.[27] The equivalent of these provisions are not contained in the UNCITRAL Model Law, nonetheless, a shortcoming of the EC Convention is that it does not apply to consumer contracts.

According to paragraph 71 of the Explanatory note on the EC Convention, the rationale for the total exclusion of consumer contracts from its sphere of application, is that a number of provisions in the EC Convention are inappropriate for consumer contracts. These provisions are found in article 10, paragraph 2 and provides for the presumption of receipt of an e-communication from the moment it becomes capable of being retrieved by the addressee. It was felt that it would be burdensome for

---

25 EC Convention art 2(1)(a).

26 EC Convention art 2(1)(b) these transactions include "foreign exchange, inter-bank payment systems, inter-bank agreements, or clearance and settlements systems relating to securities or other financial assets or instruments; the transfer of security rights in sale, loan or holding of or agreement to repurchase securities or other financial assets or instruments."

27 EC Convention arts 11, 12 & 14.

consumers to regularly check their e-mails or know the difference between regular mails or spam. Other reasons adduced include issues relating to the use of standard terms by service providers, and the complexities involved in the treatment of errors.[28]

These reasons notwithstanding, it is submitted that the EC Convention ought also to have applied to consumers with the express exclusion of these few provisions about which the Commission had concerns.[29] Nevertheless, while some member states of the UN have the EC Convention in force in their States,[30] the US is an example of a country whose e-transaction law is a combination of the EC Convention and the UNCITRAL Model Law and applies to consumer contracts.[31]

3.3 The UNCITRAL Model Law on Electronic Commerce 1996

3.3.1 Background

The UNCITRAL Model Law was prepared as a response to changes in business interactions whereby parties were attracted to the use of computers and other modern techniques to transact business in view of the ease of e-communication. E-transactions gave rise to more complications as they involved a greater volume of cross-border trade and were shrouded in uncertainty regarding, for example, the validity of e-contracts; the evidential value of data and e-signatures; and the application of the rules of time and place of contracting to online contracts.[32] An

28 Explanatory note on EC Convention para 73.

29 For further discussion of the Convention see Eiselen (2007) *PELJ/PER 48*; Kilian and Boss *Electronic Communications in International Contracts* 75.

30 The EC Convention is in force in Fifteen member states of the UN namely, Azerbaijan; Bahrain; Benin; Cameroon; Congo; Dominican Republic; Fiji; Honduras; Kiribati; Mongolia; Montenegro; Paraguay; Russian Federation; Singapore and Sri Lanka see "Status: United Nations Convention on the use of Electronic Communications in International Contracts (New York, 2005) available at www.uncitral.un.org (date of use: 21 January 2021).

31 The US legislation on electronics transactions (Uniform Electronic Transactions Act-UETA) implements the provisions of the EC Convention.

32 See Pistorius (2002) XXXV *CILSA* 129-131; Pistorius (1999) *SA Merc LJ* 282; Daniel (2004) *Santa Clara Computer and High Technology LJ* 328-30; Coetzee (2004) 15/3 *Stell LR* 502-503; Department of Communications "Green Paper on Electronic Commerce for South Africa - for public discussion" Executive Summary, Chapters 2 & 3 available at https://www.westerncape.gov.za/text.pdf (date of use: 28 June 2018); Dugan 2001 *New Zealand*

international response was required as the new technology offered no legislative support for businesses and consumers – only self-regulation and piecemeal regulations in some jurisdictions were available.[33] Thus, the UNCITRAL Model Law was adopted in 1996 in furtherance of the mandate of the UNCITRAL "to promote the harmonisation and unification of international law so as to remove obstacles caused by inadequacies and divergences in the law affecting trade."[34]

The UNCITRAL Model Law is a framework law with no intention to provide for all the aspects of the use of modern communication techniques in e-commerce.[35] Adoption of the law is not obligatory, but it is intended to promote the use of e-communication and the enactment of relevant legislation where there is none.[36] It is actually a guide for legislators to follow in enacting appropriate legislation for e-commerce.[37]

Furthermore, the UNCITRAL Model Law aims at creating a more certain legal environment for e-commerce[38] through the provision of functional equivalents[39] and without emphasis on technicalities.[40] The UNCITRAL Model Law may also be useful in the interpretation of other international instruments containing provisions that are capable of impeding the adoption of e-transactions such as requiring that documents must be in writing.[41] In summary, the Model Law is an international guideline, a model, and a standard for nations to adopt when drafting their national legislation.

LJ 483; Watnick 2004 *Baylor LR* 176; Todd *E-Commerce Law* 169-82; Thomsen and Wheble *Trading with EDI* 135-43.

33 Faria "Legal harmonisation" 4.

34 Ibid.

35 Faria "Legal harmonisation" 13; for further discussion see Pistorius (2002) XXXV *CILSA* 133.

36 Guide to enactment UNCITRAL Model Law para 124.

37 Guide to enactment UNCITRAL Model Law para 2.

38 Pistorius (2002) XXXV *CILSA* 130, see also Glatt (1998) 1 *JILT* 6.

39 Herman G "Establishing a Legal Framework for Electronic Commerce: The work of the United Nations Commission on International Trade (UNICTRAL)" paper presented at WIPO International Conference on "Electonic Commerce and Intellectual Property" Geneva 14-16 September 1999 at 2.

40 Ibid at para 141.

41 Guide to enactment UNCITRAL Model Law para 5.

3.3.2 Provisions

The UNCITRAL Model Law is divided into two parts. The first addresses the general aspects of e-communication such as the legal recognition of data messages, the application of legal requirements to data messages, and the communication of data messages. Part Two addresses specific areas in e-commerce such as the carriage of goods and transport documents. The first part of the UNCITRAL Model Law is more relevant to consumer protection and is considered further below.

3.3.2.1 Scope

One major achievement of the UNCITRAL Model Law is its flexibility in defining data. In article 2 of the UNCITRAL Model Law a data message is defined as "information generated, sent, received, or stored by electronic, optical or similar means…" This open-ended provision for "similar means" creates room for the application of the law to new techniques in the future.[42] It is submitted that since the adoption of the UNCITRAL Model Law, technology has improved, especially in the area of m-commerce, so that although it does not specifically refer to m-commerce, the provisions will apply *pari passu* in view of its anticipated reference to future technologies. The UNCITRAL Model Law applies to any kind of information in the form of a data message, whether in local or international communications. States are, however, permitted to limit its application to international data messages.[43] While it is possible to restrict the scope of the UNCITRAL Model Law to international communications, it should be noted that in some jurisdictions – most notably in federal states, it might be near impossible to distinguish between international and domestic trade.[44] States are therefore advised to be careful whenever they try to apply such a limitation so that it might not constitute a barrier to the use of the UNCITRAL Model Law.[45]

---

42 See further Guide to enactment UNCITRAL Model Law paras 8 & 31; see also Gregory (1999) 32 *CBLJ* 84-104.

43 Guide to enactment UNCITRAL Model Law para 28.

44 Ibid.

45 Guide to enactment UNCITRAL Model Law para 29.

In examining the scope of the UNCITRAL Model Law, the term "commercial" is given a very broad meaning to cover all non-contractual or contractual commercial transactions, which includes:

> any trade transaction for the supply or exchange of goods or services; distribution agreements; commercial representation or agency; factoring; leasing; construction of works; consulting; engineering; licensing; investment; financing; banking; insurance; exploitation agreements or concessions; joint ventures and other forms of industrial or business cooperation; and the carriage of goods or passengers by air, sea, rail or road.[46]

States are also enjoined to extend the scope of the law to protect non-commercial transactions,[47] and to allow the provisions of other laws which provide a wider coverage for consumer protection.[48] States may also define a consumer within the provision of their laws.[49] Furthermore, the law applies to e-communications such as the EDI, e-mail, and less advanced communication techniques such as telex and telecopy,[50] and to future technologies in e-communication. It applies to all forms of contract for both consumers and businesses.[51] The Model Law upholds the principle of party autonomy.[52] Under the provisions of the UNCITRAL Model Law, parties are free to vary the terms of their agreements, save in respect of conditions relating to the use of data messages contained in articles 5-10 of the Model Law.[53]

3.3.2.2 Application of legal requirements to data messages

The law provides ample legal protection for messages generated by electronic means.[54] Data messages generated by parties themselves or by AMS are valid and

46 UNCITRAL Model Law art 1.
47 Guide to enactment UNCITRAL Model Law para 26.
48 Guide to enactment UNCITRAL Model Law para 27.
49 Ibid. Applicable law here is understood to refer to consumer protection law on which the enacting state currently relies. This position, therefore, is not conclusive as to who a consumer is under the Model Law. Recourse must be had to the intention of the Model Law to provide as much coverage as possible for the protection of e-commerce consumers, see para 26 of the Guide to enactment of the UNCITRAL Model Law which provides that nothing in the UNCITRAL Model Law should prevent a state from extending the scope of application of the Model Law.
50 Guide to enactment UNCITRAL Model Law para 7.
51 UNCITRAL Model Law art 1; see also Guide to enactment UNCITRAL Model Law para 26.
52 UNCITRAL Model Law art 4; Guide to enactment UNCITRAL Model Law para 44.
53 UNCITRAL Model Law art 4.
54 Amro (2016) 20 *Vindobona Journal of International Commercial Law & Arbitration* 22-23.

enforceable.[55] Traditionally, documents are required to be in writing and signed, and although there is widespread use of e-communication for e-contracting, certain legal rules continue to demand the use of writing for specific documents or transactions.[56] One of these impediments is the requirement that for a document to be admissible as best evidence, the document should be an original or a copy of a public document certified as a true copy. The Model Law recognises these impediments and in paragraph 48, eleven reasons for the use of written documents are stated. The reasons include parties' desire to have tangible evidence, legibility, reproduction, accounting, easy storage, and proof of intent of parties, amongst other reasons.

By virtue of the provisions of the UNCITRAL Model Law, these requirements are now met when they are in the form of a data message.[57] A data message fulfils the requirement of writing; provided it is expressed in a medium that is accessible for future use, save in exceptional cases where the law specifies "writing" on paper as a requirement.[58] The UNCITRAL Model Law requires that data should be readable, capable of being interpreted, and available for subsequent use both by humans and the machine processing the information. The legal questions raised here go to the issues of reliability, traceability, originality, and alterability. Data messages can be reliable and traceable, but can they not be altered? According to Sprowl,[59]

> once information has been kept as a computerised record, later alterations can no longer be detected easily, as no tell-tale traces are left when one presses the DELETE key of a computer and part of or the whole of the record concerned is instantly erased.

Again, since all computer printouts turn out exactly the same, which would then be regarded as the "original" under the best evidence rule?[60]

---

55 UNCITRAL Model Law arts 5 & 13.

56 Davies "The development of laws" 1; Fry (2001) 37/2 *Idaho Law Review 241*.

57 Wang (2015)2 *Journal of Business Law* 96.

58 Guide to enactment UNCITRAL Model Law para 51.

59 Sprowl and Maggs *Computer Applications in the Law* 4-5.

60 All computer printouts made by a uniform process are originals whereas subsequent copies made out of the original printout will be duplicates and as such, secondary evidence of the original copy, see s 86(4) of the Evidence Act.

For computer-generated records, it is posited that such records qualify as best evidence as they constitute the only record of a certain transaction. This aside, many computer-generated records have no underlying documents from which the information can be obtained as they were created by the computer system itself.[61] Such records include, for example, computer-generated statements of account. Different jurisdictions provide for the admissibility of computer records. Over time, the emphasis has shifted from the admissibility of computer records to their evidential weight. Evidential weight can be assessed based on how reliable the data message was created, stored or communicated; as well as the integrity of its source.[62]

The UNCITRAL Model Law also addresses the function of a signature in the authentication of documents. Although not defined in the Model Law, an e-signature is defined in article 2 of the UNCITRAL Model Law on Electronic Signatures[63] as

> data in electronic form in, affixed to, or logically associated with a data message, which may be used to identify the signatory in relation to the data message, and to indicate the signatory's approval of the information contained in the data message.

An e-signature has also been defined as "letters, characters or symbols manifested by electronic or similar means and executed or adopted by a party with intent to authenticate writing."[64]

A signature performs two principal functions, first, it attests to the identity of the parties, and secondly, it evidences their intention to be bound by the terms of an agreement.[65] E-signatures do not only perform the above functions, they also have the advantage of showing alterations after the signature has been affixed or appended, thus providing a high level of authenticity for the document.[66] Under the UNCITRAL Model Law on E-

---

61 Ver Der Merwe *Computers and the Law* 207.

62 UNCITRAL Model Law art 9.

63 The underlying principles on e-signature in art 7 of the Model Law are expanded by the UNCITRAL Model Law on Electronic Signatures, adopted 5 July 2001, see the Preamble.

64 Blyth (2005) 11 *Richmond Journal of Law & Technology* 1 available at http://jolt.richmond.edu (date of use: 18 April 2019).

65 Guide to enactment UNCITRAL Model Law para 56; see Zemnick (2001) 76/3 *Chicago-Kent Law Review* 1972.

66 See UNCITRAL Model Law on Electronic Signatures art 6(3)(c); see also Erdle "On-line Con-

Commerce and the UNCITRAL Model Law on Electronic Signatures, there is no specified or mandatory technology or media prescribed for the processing of an e-signature thus ensuring technological neutrality. Some laws may, however, require signatures to be preceded by the signature of witnesses, or the fixation of a "stamp, perforation, or a printed letterhead".[67] These requirements can all be met using an e-signature.

Agreements concluded in an e-contract can also be authenticated by "system rules or technical standards." Most internet contracts are authenticated by the use of web agreements where the "I agree" button is clicked to signify consent and intent to be bound. Some national laws have proposed authentication authorities for the establishment of secure e-signatures.[68] What has, however, been achieved, is the removal of the requirement of a hand-written signature to authenticate documents, as the use of e-documents or agreements no longer require hand-written signatures. Any form of an authenticated mark or process that links the user to the document and which shows that the user intends to be bound to the terms or content of that document or agreement is sufficient.[69]

In electronic records where every printed copy appears as an original, the requirement of originality is met where it is certain that the content of the copy has not been altered since its creation and that the data can be displayed whenever appropriate.[70] The addition of necessary information such as an electronic certificate, notarisation, or similar additions at the beginning or end of a document through computer inputs, does not affect the originality of a document.[71] It is opined that e-documents could be downloaded, optically imaged or photographed by parties to ensure their integrity for

tracts: Electronic Creation of Effective Contracts" (2001) available at www.dww.com/articles/online (date of use: 08 October 2020); Angel (1999) *JILT* 4.

67 Guide to enactment UNCITRAL Model Law paras 53 and 54.

68 See for instance the South African ECTA s 37.

69 This position was upheld in the case of *WS Tankship II BV v The Kwangju Bank Ltd and another* (2011) EWHC 3103 available at www.uk.practicallaw.thomsonreuters.com (date of use: 20 June 2019).

70 Guide to enactment UNCITRAL Model Law para 67.

71 Ibid.

reference purposes. Also, whoever is placed with the obligation of retaining a data message should do so directly, through an intermediary or through the services of a third party under agreed terms.[72]

Article 5 *bis* which was introduced into the UNCITRAL Model Law in 1998, provides for incorporation by reference of any information in whatever format including paper communication, "databases, code lists, glossaries,"[73] or codes in the data message. Any information can be incorporated into a data message through a URL which directs the reader to the referenced document. A claim that information forms part of an e-message will only be available to the claimant under the following three conditions:

(a) that the reference clause was inserted in the data message;[74]
(b) that the document being referred to is actually known by the party against whom the reference document is to be relied on;[75]
(c) that the reference document is accepted, in addition to being known by the other party.[76]

Where it is shown that a reference actually forms part of a data message, such as terms of use or a licence enclosed in a purchase of software, the user will be bound to the terms of such usage.[77] The UNCITRAL Model Law, however, leaves room for states who may desire to exclude some documents from the application of the law, to do so, when it comes to the requirements of signature and originality.

3.3.2.3 Communication of data messages and electronic contracts

Chapter three of part one of the UNCITRAL Model Law examines the validation of e-contracts. The preceding paragraphs deal with the validation of data messages through the adoption of a functional equivalence approach. This approach now

72 Guide to enactment UNCITRAL Model Law para 75.
73 Guide to enactment UNCITRAL Model Law para 46.
74 Guide to enactment UNCITRAL Model Law para 46-7
75 Ibid.
76 Ibid.
77 See the cases of *ProCD Inc v Zeidenberg* 86 F 3d 1447 (Court of Appeal 7th Circuit 1996) and *MA Mortenson Co v Timberline Software Corporation* 998 P 2d 305 (Wash Supreme Court 2000) discussed on para 6.5.1.9 page 262.

recognises the functional equivalence of data messages and paper-based writing in different jurisdictions.[78]

Besides paper-based contracting, electronic contracting is another way of reaching agreements, and is valid on its own force.[79] They follow the same rules on contract formation with additional safeguards in terms of issues which are peculiar to the online space.[80] It is submitted that emerging rules on e-transactions are merely a refinement of existing substantive law, and not a replacement. This is particularly so as one of the objects of the UNCITRAL Model Law is not to impose the use of e-contracting but to validate it.[81]

In *Druet v Girouard*[82] what was at issue was whether e-mail messages and the requirement of an e-signature was met and sufficient to enforce the sale of a residential condominium unit under the law in New Brunswick.[83] In this case, two private individuals exchanged seven e-mails in two days concerning the sale of a condominium unit. On the e-mails the seller indicated her names in different forms and added her phone number but the buyer's name was not written in his e-mails.[84] At some point the seller decided not to go ahead with the transaction, but the motion Judge held that all the essential terms of a valid contract were in the e-mails. The sale was therefore validated. The vendor was dissatisfied with the judgement of the court and sought leave of the Court of Appeal of New Brunswick, to appeal.[85] The Court of Appeal in its analysis agreed that the requirement of writing was met by the use of the

78 Guide to enactment UNCITRAL Model Law para 16; see also Lodder "Electronic Contract and Signatures" 4.

79 Donnie and William (2000) 26 *RCTLJ* 269; Harvey *Internet.law.nz* 348; Van der Merwe et al *Contract* 61-4; *Bok Clothing Manufacturers (Pty) Ltd v Lady Land Ltd* 1982 (2) SA 565 (C) 569E; *Gincrete (Pty) Ltd v Scherringhuisen Construction (Pty) Ltd* 1996 (2) SA 682 (N).

80 Pompian (1999) 85 *Virginia LR* 1479 cited in Faria (2004) 16 *SA Merc LJ* 535.

81 Guide to enactment UNCITRAL Model Law para 79.

82 *Druet v Girouard* CLOUT case 1197, 2012 NBCA 40 (hereafter the *Druet* case).

83 The *Druet* case para 1.

84 The *Druet* case paras 6-12.

85 The *Druet* case para 1.

e-mails between the parties[86] and that the requirement of using an e-signature is broad enough to include the use of any attached or attributed e-communication to a message or an e-mail.[87] However, the Court allowed the appeal and set aside the decision of the motion judge, because in the opinion of the court the parties did not show sufficient intention to enter into a legal relationship in respect of the sale of the condominium at issue.[88]

From this case, it is submitted that all contracts must follow the rules of offer and acceptance, and that a counter-offer cannot of itself constitute an acceptance. Receipt of a data message in the absence of a valid agreement does not in itself translate into a valid contract. E-transaction rules are complementary to substantive elements that could void a contract. These elements include the concepts of "offer," "acceptance," "invitation to treat," "time and place of dispatch," as well as requirements relating to the capacity of contracting parties, consideration, the legality of the contract, and so on. A valid and binding contract is *ipso facto* concluded when an offer is unconditionally accepted by the offeree in the absence of any vitiating elements.[89]

Another major hurdle in e-contracts is the adaptation of traditional rules of contract formation regarding where and when a contract is concluded, to the electronic environment.

Under the conventional rules of contract, the time and place of dispatch of an offer and the place of acceptance are trite in the determination of jurisdiction and choice of law. The position, although complicated, is not different under the electronic regime. The

86 The *Druet* case para 3.

87 The *Druet* case paras 26-27.

88 The *Druet* case paras 51-54.

89 On the general principles of contract formation, see Sagay *Nigerian Law of Contract* 6,13; Van der Merwe et al *Contract* 46-7; Christie & Bradfield *Law of Contract* 30-1; Pistorius (1999) 11 *SA Merc LJ* 285-7; Pistorius (2002) XXV *CILSA* 138-9; Lloyd *Legal Aspects of the Information Society* 233-4; Eiselen and Bergenthal (2006) 39 *CILSA* 214-5; *Watermeyer v Murray* 1911 AD 61, 70; *Reid Brothers (SA) Ltd v Fischer Bearings Co Ltd* 1943 AD 232-241; *Estate Breet v Peri-Urban Areas Health Board* 1955 (3) SA 523 (A) 523(E); *Collen v Reitfontein Engineering Works* 1948 (1) SA 413 (A) 420. See also, Rowland, Kohl and Charlesworth *Information Technology Law* 448.

UNCITRAL Model Law provides rules on the time and place of dispatch and receipt in e-transactions which could effectively be likened to the postal or mail-box rule.

The UNCITRAL Model Law provide as follows:[90]

> (1) Unless otherwise agreed between the originator and the addressee, the dispatch of a data message occurs when it enters an information system outside the control of the originator or of the person who sent the data message on behalf of the originator.
> (2) Unless otherwise agreed between the originator and the addressee, the time of receipt of a data message is determined as follows:
> (a) If the addressee has designated an information system for the purpose of receiving data messages, receipt occurs:
> (i) At the time when the data message enters the designated information system; or
> (ii) If the data message is sent to an information system of the addressee that is not the designated information system, at the time when the data message is retrieved by the addressee;
> (b) If the addressee has not designated an information system, receipt occurs when the data message enters an information system of the addressee.

It must be noted that dispatch and receipt of a data message are instantaneous when the data message leaves the information system of the originator to the information system of the addressee, or the addressee's designated information system.[91] A data message that fails to enter the addressee's information system for whatever technical reasons (or enters the system but is not accessible due to unsupported file formats or due to corruption of the file), is not considered as having been received.[92]

The principles governing offer and acceptance and, in this case, dispatch and receipt, are tied either to the "mail-box" rule or the rule applicable to "instantaneous" communication. The question of which rule will apply to e-commerce contracts depends on whether the exchange of communications is instantaneous. Instantaneous or direct communications can be applied in face-to-face meetings where the parties are in the presence of one another, or through a telephone conversation. On the other hand, the mail-box rule, or the postal rule, applies where there is dispatch of

90 UNCITRAL Model Law art 15.
91 Guide to enactment UNCITRAL Model Law para 101.
92 Guide to enactment UNCITRAL Model Law para 104.

communication by the parties. Under the United States Restatement (second) of the Law of Contract, the mail-box rule provides that

> an acceptance made in a manner and by a medium invited by an offer, is operative and completes the manifestation of mutual assent as soon as it leaves the offeree's possession, without regard to whether it ever reaches the offeror.[93]

As earlier stated, under the application of the UNCITRAL Model Law, receipt is deemed to have taken place when a data message enters the recipient's information system. In the case of *Paccar Financial Services Itee v Kingsway, General Insurance Company*,[94] a company concluded a contract for the lease of a truck subject to the condition that the lessee (the appellant in this case) would take out insurance coverage against theft of the truck.[95] The notice to install an anti-theft system was sent to the appellant by telefax[96] although there was a claim by a staff of the appellant that the log was not checked.[97]

The Court based its findings on the evidence of the insurance company which showed proof that the letter was successfully dispatched to the lessor.[98] The court referred to article 31 of the e-communications law of Quebec which provides that

> a technology-based document is presumed received or delivered where it becomes accessible at the address indicated by the recipient as the address where the recipient accepts the receipt of documents from the sender or at the address that the recipient publicly represents as the address where the recipient accepts the receipt of documents, provided the address is active at the time of sending.[99]

The court therefore denied the appellant's appeal with costs.[100]

---

93 American Law Institute Restatement (Second) of contract (Washington, DC American Law Institute, 1979) s 63(a).

94 *Paccar Financial Services Itee v Kingsway, general insurance company* 2012 QCCA 1030 (can LII) available at http://www.uncitral.org/clout/data/can (date of use: 28 June 2020) (hereafter *Paccar Financial Services* case).

95 *Paccar Financial Services* case para 4.

96 *Paccar Financial Services* case paras 7,8,9.

97 *Paccar Financial Services* case para 11.

98 *Paccar Financial Services* case para 10.

99 *Paccar Financial Services* case para 12.

100 *Paccar Financial Services* case para 25.

On rules governing dispatch, the UNCITRAL Model Law places emphasis on the place of business of the parties and not the location of the information systems as this may change without the knowledge of a contracting party.[101]

The UNCITRAL Model Law also provides for acknowledgement of receipt of data messages, although such an acknowledgement does not amount to consent or intention to be bound. But where parties request acknowledgement of receipt without indicating a particular mode of receipt, the law provides that a response, whether automated or otherwise, or the conduct of the addressee, is sufficient to meet the requirement. However, where acknowledgement of a message is required and there is none, it will be regarded as though the message was not sent.[102]

In addition to the requirement of recognising data messages for the conclusion of a contract, provision is also made generally for the validity, and enforceability of information transmitted by electronic means. Such information could include, but is not limited to commercial notices, offer and acceptance.[103]

3.3.2.4 Exclusions

The approach used in the UNCITRAL Model Law is geared towards a general application which is, as far as possible, free from exclusions. It is feared that numerous exclusions may raise obstacles to the development of modern communication technology.[104] There might, however, be exclusions in national laws with respect to articles 6, 7, and 8 dealing with writing, signature, and originality. Under these articles, national laws could provide certain exclusions for certain situations, such as warnings of specific or actual risks. Such exclusions could be in respect of warnings to be placed on some products, and also in respect of a cheque.[105] Further exclusions may also arise from the provisions of articles 11, 12, 15 and 17 dealing with

101 UNCITRAL Model Law article 15(4).
102 UNCITRAL Model Law art 14.
103 UNCITRAL Model Law art 11; Guide to enactment UNCITRAL Model Law para 81.
104 Guide to enactment UNCITRAL Model Law para 52.
105 Guide to enactment UNCITRAL Model Law para 51.

contract formation, the use of data messages especially for transport documents, and exclusions regarding the time and place of dispatch and receipt of data messages.

3.3.3 Limitations

The uniqueness of the UNCITRAL Model Law notwithstanding, there are important limitations which impact negatively on the adequate protection of e-commerce consumers.

(a) The UNCITRAL Model Law is not a binding legislative act and therefore does not bind member states which in turn, means, that its implementation is optional.

(b) There are no specific consumer-protection measures dealing with rights of consumers.

(c) There are no comprehensive provisions on certain aspects of e-contracting such as “invitation to treat” or “pre-offer,” “offer,” and “acceptance.”

(d) There are no clear provisions on the protection of internet intermediaries such as ISPs and rules on when they may be held liable for infringements. This lack of clear rules creates uncertainties for consumers in the bid to determine their rights.

(e) The UNCITRAL Model Law is silent on the issue of jurisdiction on the internet, although the provisions on the location of the parties are relatively clear. The UNCITRAL Model Law tends to rely on other laws on this issue. However, it would be a more comprehensive model if it were to provide clear rules on jurisdiction in e-consumer contracts.

(f) There are no standards which address the likelihood of errors during an e-transaction between natural and juristic persons without the use of e-agents. Input errors in consumer transactions occur frequently, a model provision on the resolution of input errors in e-consumer contracts in all circumstances would afford the e-commerce consumer, better protection.

(g) There are no requirements requiring suppliers and service providers to disclose certain information about themselves and their businesses online. Anonymity on the internet is a fundamental issue which the law must resolve in order to protect the e-commerce consumer from fraud. With clear information on the physical and electronic address of a business, a consumer can verify and rely on the information for the purposes of concluding a transaction. Important information requirements on the nature of goods and attached obligations of both supplier and consumer and information on interoperability of software and hardware as well as limitations on use of any product, if any are all unaddressed.

(h) It is not enough that terms which are incorporated into online agreements are acceptable because they have been properly referred to; there should be provisions guiding against the use of unfair terms. Incorporated terms should also be downloadable or otherwise accessible.

(i) The UNCITRAL Model Law does not provide for the privacy of consumers or create options which enable them to opt in or out of unsolicited commercial communications sent directly to them. There is an absence of stringent rules prohibiting or limiting inertia selling and spam. In the same vein, there are no specific rules regulating e-communications directed to children, or vulnerable persons.

(j) The provision for retention of data messages is unclear as to who bears the responsibility to retain data according to applicable laws. It appears that the responsibility is charged to the originator of the data message and not the third party who provides the service. This obligation appears too remote. Messages should be capable of retention to serve as evidence of communication between the parties as e-commerce consumers may have to rely on their communication with suppliers in exercising their rights.

(k) Although the UNCITRAL Model Law attempts to provide for future technologies, and that can be safely assumed to cover m-commerce, this “success” cannot be sustained in the face of current challenges raised by the use of electronic single-window facilities and electronic transferable records which are not

addressed in the law. These current challenges are sometimes experienced in consumer contracts and a vacuum in the law could expose consumers to inadequate protection.

(l) Misleading and deceptive advertisements are not dealt with in the Law.

(m) The principle enunciated by the legal *dictum, ubi jus, ibi remedium,* does not feature in the UNCITRAL Model Law as there is no provision for an effective system for redress. E-commerce consumers will be better protected when they are able to access redress timely and effectively when the need arises.

3.3.4 Implementation

This chapter of the study has shown the relevance of the UNCITRAL Model Law to consumer protection. The Model Law is expected to be implemented in national legislation of all UN countries either as a single statute or in any relevant piece of legislation.[106] In effecting its implementation, states are advised to interpret the provisions of the UNCITRAL Model Law in the light of its international character so as to ensure a uniform effect in those countries whose domestic law on e-commerce are modelled after the Model Law.[107] The Model Law is a set of guiding principles and can only be enforced at the national level by states.[108] However, there are no proposed structures for the enforcement of e-commerce law as implemented by states.

3.3.5 Summary

From the study of the UNCITRAL Model Law the conclusions listed below can be drawn.

(a) The UNCITRAL Model Law was the first international document to address the legality of data messages and has led to the development of future work in the field.

106 Guide to enactment UNCITRAL Model Law para 10.
107 Guide to enactment UNCITRAL Model Law para 42.
108 In chapter three the nature of the Model Law as a framework was explained thus it cannot of itself be enforced against any organ or person, see particularly para 3.3.

(b) The Model Law provides for a wide coverage of the use of data messages. This wide scope is capable of capturing both existing forms of data messaging, including mobile services, and future technologies. This foresight makes the Model Law unique and relevant to electronic consumer contracts.

(c) With data the requirements of writing and signature are satisfied[109] especially when adopting the doctrine of a functional equivalence which was first propounded in the UNCITRAL Model Law.[110] E-documents now serve all purposes including purposes such as e-invoice and e-notarisation.[111] E-documents are also admissible in evidence.[112]

(d) It is worthy of note that contracts can be formed using all forms of electronic communications including the use of e-mails[113] while contracts entered into with the use of e-agents or automated robots are valid and enforceable.[114] Offer and acceptance effectively take place through e-mails[115] and by consenting to terms and agreements online.[116] Like conventional contracts, terms can be incorporated into contracts by a link or reference provided the consenting party is aware of the existence of such terms and his or her duty to be bounded.[117] Parties are also at

---

109 UNCITRAL Model Law arts 6-7; E-commerce Directive art 9; E-signatures Directive arts 1 & 2; ETA ss 8-10; AU Convention art 6; ECTA ss 12-13; UETA s 7.

110 Guide to enactment UNCITRAL Model Law para 16; Lindholm and Maennel "Directive on Electronic Commerce" (2000/31/ec)" 21-22.

111 AU Convention art 6(5); ECTA s 19; UETA s 11.

112 UNCITRAL Model Law art 9; ECTA ss 14-15; AU Convention art 6(6); UETA s 13.

113 Donnie and William (2000) 26 *RCTLJ* 269.

114 UETA s 14; similarly contracts with AMS are valid in the EU see E-commerce Directive art 11(1) which enables contract formation with an AMS provided an invoice or a document in respect of the transaction is made available to the consumer who in turn must acknowledge same for the purpose of fixation and reproduction. In South Africa contracts concluded with AMS are enforceable where however, the contract is between a natural person and an AMS there must be provision for the natural person to correct errors before the contract is concluded in order for the contract to gain validity see ECTA s 20; a similar provision is made in ETA ss 15C & 15D.

115 The Druett case is an example of a case where the courts gave recognition to an e-mail communication in a contract agreement. This case was discussed in chapter 3 of this study, see *Druet v Girouard* 1197: MLEC (5); 6(1); (7) 2012 NBCA 40.

116 See *MA Mortenson Co v Timberline Software Corporation* 998 P 2d 305-Wash Supreme Court 2000 discussed in Chapter 6; Donnie and William (2000) 26 *RCTLJ* 269.

117 UNCITRAL Model Law art5 *bis*; ECTA s 11(2); Jacobs (2004) 16 *South African Mercantile Law Journal* 558.

liberty to alter terms of their contracts[118] where consumers are not disadvantaged by terms which may be unfair or unconscionable.[119]

(e) The Model Law does not limit its application by technical standards; it is technologically neutral.

(f) There is room for parties to vary the terms of their contract save as regards legal recognition of data messages.

(g) Automated transactions are recognised and enforceable.

(h) The Model Law applies to consumer contracts.

3.4 United Nations Guidelines for Consumer Protection 2015

The UNCITRAL Model Law and the EC Convention in the protection of consumers compliments the United Nations Guidelines for Consumer Protection (UNCP Guidelines).[120] The UNCP Guidelines apply to B2C transactions[121] and comprise of policies with minimum objectives which member states are expected to achieve for adequate consumer protection.[122] The UNCP Guidelines sets out principles; guidelines and measures for international cooperation. The principles address fair business practices; education; data protection; and effective dispute resolution.[123] There is specific emphasis on the protection of e-commerce consumers commensurate to the protection enjoyed by conventional consumers.[124] The UNCP Guidelines further provides for an intergovernmental group of experts whose responsibility it is to implement an institutional machinery to guide member states in the attainment of the overall objectives of the Guidelines.[125]

---

118 UNCITRAL Model Law art 4; Parties can formulate agreeable terms for their transaction ECTA s 21; UETA s 5(d).

119 CPR para 6; OECD *Toolkit for protecting digital consumers* 24.

120 United Nations Guidelines for Consumer Protection 2015 first adopted in 1985, expanded in 1999 and revised and adopted by the General Assembly in resolution 70/186 of 22 December 2015; see further Lianos *et a*l "The global governance of online consumer protection" 11.

121 UNCP Guidelines para 2.

122 Harland (1991) 33/2 *Journal of the Indian Law Institute* 189.

123 UNCP Guidelines para 4.

124 UNCP Guidelines paras 95 & 97.

125 Ibid.

3.5 UNCITRAL Model Law on Electronic Transferable Records 2017

The UNCITRAL Model Law does not provide for e-transferable records, this shortcoming has been addressed to meet current developments in e-transactions by the adoption of the UNCITRAL Model Law on Electronic Transferable Records (MLER).[126] The MLER applies to all e-transferable records with the exception of securities such as shares, bonds, and other investment instruments.[127] The MLER defines a transferable document or instrument as one

> issued on paper that entitles the holder to claim the performance of the obligation indicated in the document or instrument, and to transfer the right to performance of the obligation indicated in the document or instrument through the transfer of that document or instrument.[128]

The requirement of an e-transferable record is met if the electronic record contains required information that retains its integrity.[129]

The MLER provides that an e-transferable record shall not be denied legality because it is in an electronic form.[130] The records also enjoy the functional equivalence of writing and signature.[131] It is provided that there shall be no discrimination against a foreign e-transferable record. Article 19 provides that e-transferable records used abroad shall also be treated as e-transferable records used within jurisdiction without discrimination. The MLER is very relevant as the legal status of electronic instruments which are used in the conduct of business are always relevant to consumer protection since the law would as a principle, protect the interest of parties to a transaction. The absence of law in any context creates an opportunity for fraud, lack of enforcement and undue hardship.

126 UNCITRAL Model Law on Electronic Transferable Records adopted 13 July 2017.
127 MLER art 1.
128 MLER art 2.
129 MLER art 10.
130 MLER art 7.
131 MLER arts 8-9.

3.6 Conclusion

While it is acknowledged that the bedrock of consumer protection laws for online users was established in the UNCITRAL Model Law, there is no gainsaying that much more is needed for an effective consumer protection regime. It is essential that future work is undertaken to modify the UNCITRAL Model Law to meet current developments that are relevant to the protection of e-commerce consumers. The underlying advantage of the UNCITRAL Model Law in comparison with the EC Convention lies in its broader scope of application to consumer contracts. As noted in paragraph 3.2 above, the EC Convention does not apply to consumer contracts. However, the success of the UNCITRAL Model Law is evidenced by the overwhelming pieces of legislation on e-commerce modeled on its provision.[132] Exceptions are the EU CRD,[133] which stands out for its highly elaborate and innovative provisions. For jurisdictions where both the EC Convention and the UNCITRAL Model Law have been adopted – for example, the COMESA – the EC Convention will be applied in international commercial transactions, while the Model Law will be extended to those areas which the EC Convention does not provide for; such as consumer contracts, evidence, retention of data messages, originality, et cetera.[134]

One of the limitations of the UNCITRAL Model Law in not providing for dispute resolution has, however, received attention from the UN in its subsequent work. The Secretariat has proposed an integrated ODR system design based on generic rules which could apply to all forms of e-transactions. The Secretariat advocates out of court settlements, especially by ODR which is convenient and cheap.[135] Technical Notes on

---

132 See Pistorius (2002) XXXV *CILSA* at 132 n 17 where she provides a list of countries whose e-transaction laws are modelled on the UNCITRAL Model Law on e-commerce, see also the UN-CITRAL website where it is stated that legislation based or influenced by the UNCITRAL Model Law has been adopted in 72 member states in a total of 151 jurisdictions, available at www.uncitral.org (date of use: 28 October 2020).

133 The CRD is discussed in Chapter 4 of this study, see para 4.5.

134 COMESA Model Law, Guide to Enactment para 26.

135 UNCITRAL "Possible future work on Online Dispute Resolution in Cross-border Electronic Commerce Transactions" 43rd Session 26 May 2010 n 2; see also UN "Report of the United Nations Commission on International Trade Law" 47th Session July 2014 AT 19 and 25.

ODR have been adopted by the resolution of the UN General Assembly and states are requested to support their use.[136]

In chapter 4 of this research, the protection of e-commerce consumers is examined in Europe with specific reference to the OECD. The chapter also contains a study of e-commerce rules and e-commerce consumer protection regime that is available in Australia.

136 On 13 December 2016 the UN General Assembly adopted the *Technical Notes on Online Dispute Resolution of the United Nations Commission on International Trade Law*.

CHAPTER FOUR

REGIONAL PROTECTION OF ELECTRONIC COMMERCE CONSUMERS: EUROPE AND AUSTRALIA

4.1 Introduction

With the advent of electronic consumption, consumer protection has received considerable attention in Europe especially for European countries in the EU. The EU has also embraced the challenge of creating a unified market in the light of Community objectives[1] which obliges it to eliminate obstacles which could impair free trade within member states through the coordination of certain national laws. E-commerce was hampered in Europe by fragmented legislation and legal obstacles arising from the legal requirements governing e-communications. This situation was exacerbated by uncertainties regarding the rules which member states subjected service providers from other member states.[2] Language barrier was also an impediment.[3]

A case in point was the use of monetary threshold in applying consumer protection measures for off-premises contracts including online transactions. In terms of this rule, consumer protection measures could not avail a consumer whose purchase fell below certain monetary threshold as set out in some member states.[4] This case scenario

1 Council of the European Communities, European Union Treaty, Maastricht 7 February 1992, Part 1 "Principles" arts 2 & 3.

2 Directive 2000/31/EC Recitals 5 and 6.

3 Most websites in Europe offer their services primarily in one language; only a few web-sites offer their services in two or more languages. The impact of this is that Europeans whose languages are not provided on a particular website are restricted from doing business on that website; a study of the number of websites offering two or more languages was carried out between 2002 and 2007 by the European Consumer Centre's Network. For details of the report see Jervelund "Study on the Economic impact of the E-commerce Directive" 7.

4 There was a monetary threshold ranging from 15-60 Euro in countries like Austria, Bulgaria, Estonia, Lithuania, Malta, the Netherlands, Poland, Portugal, Finland, Germany, Italy, Romania, Slovenia, Spain, Sweden, and the United Kingdom. However, in Belgium, Cyprus, Czech Republic, Denmark, Latvia, Luxembourg, France, Greece, Hungary and Slovakia consumers are always protected no matter the amount of payment involved, see European Union, *The Proposal for a Directive on Consumer Rights: Impact on Level of National Consumer Protection. Comparative Table* (2009).

presented difficulties for consumers who in practice may not be aware of the monetary thresholds that applied to e-contracts across all EU member states. Furthermore, determining the place of establishment of every website in order to apply relevant laws was impracticable for consumers. There was also disparity in areas such as the cooling-off period which varied from country to country leaving consumers confused and reluctant to purchase goods outside of their countries.[5]

In order to harmonise differing legislation and the elimination of uncertainties as regards online consumer transactions, the EU adopted some Regulations and Directives so as to establish a system of uniform community law for all EU member states in respect of e-commerce.[6]

Also relevant to e-commerce consumer protection in the EU are the recommendations and guidelines of the OECD in response to e-commerce and consumer protection. The OECD is a regional economic organisation whose member states are from Europe, Asia-Pacific and North and South America.[7] It should be noted that the European Economic Community (EEC) is represented in the OECD and takes part in their work.[8] Intrinsically it is an expectation that the EU incorporates the OECD's consumer protection principles in their legislation.[9] The OECD principles, therefore, should be

5 In Cyprus, the Czech Republic, Denmark, Estonia, Finland, Latvia, Portugal, Sweden and German consumers enjoyed a 14 calendar-day (or two-week) cooling-off period, while in some other countries the period ranged between 7-10 working days. See European Union, *The Proposal for a Directive on Consumer Rights* 7.

6 Examples of such Directives and Regulations include Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on Certain Legal Aspects of Information Society Services, in particular electronic commerce, in the Internal Market *OJL* 178, 17.7.2000 1-16; Directive 2013/11/EU of the European Parliament and of the Council of 21 May 2013 on Alternative Dispute Resolution for Consumer Disputes and Amending Regulation (EC) No 2006/2004 and Directive 2009/22/EC *OJL* 165, 18.6.2013 63-79 and Regulation (EC) No 593/2008 of the European Parliament and of the Council of 17 June 2008 on the law applicable to contractual obligations *OJL* 177, 4.7.2008 6-16, amongst others.

7 OECD "Where: Global reach" available at www.oecd.org (date of use: 05 September 2020).

8 See Supplementary Protocol No 1 to the Convention on the OECD 1960; see also OECD Convention art 13; see also OECD "European Union and the OECD" available at www.oecd.org (date of use: 20 November 2020).

9 OECD "European Union and the OECD" available at www.oecd.org (date of use: 20 November 2020).

complementary to international and regional documents on consumer protection especially in the EU.

A look at the work of the OECD alongside EU Directives and Regulations on consumer protection will therefore form part of this chapter. Thereafter, the implementation of the EU legal instruments which are basically Directives and Regulations will be discussed. EU legal instruments are implemented or domesticated by countries which are subject to EU laws, and these are EU member countries. For the purpose of this study, implementation of EU community laws by the UK will be considered. Although the UK no longer forms part of the EU,[10] their regulations and laws were drafted to give effect to EU community laws and they continue to apply until the completion of the withdrawal period which should be 31 December 2020.[11] UK is a formidable country whose laws are influenced by the EU through EU Directives and Regulations and it will be insightful to consider the level of protection which the country offers e-commerce consumers in comparison to the level of protection offered in other regions that are geographically linked to Europe, such as Australia. Although Australia is not a member of the EU, they however, have trade relations and agreement for free trade.[12]

This chapter therefore dwells on consumer protection in Europe within the context of EU community laws, legal instruments of the OECD, as well as national laws in UK and the Commonwealth of Australia. The work of the OECD is evaluated in what follows.

---

10 The UK left the EU on the 31 of January 2020 after 47 years of membership by invoking art 50 of the Treaty on EU 1992 (also known as the Maastricht Treaty), see BBC "UK no longer a member of EU" 31 January 2020 available at www.bbc.co.uk (date of use: 25 May 2020).

11 Before the exit of the UK from the EU, EU legislation could either apply directly or by domestication in accordance with s 2 of the European Communities Act 1972. However, after the exit, the UK has up to 31 December 2020 to continue to apply EU Community laws. Thereafter, some EU laws will cease to apply in the UK based on the provisions of the European Union (Withdrawal) Act 2018. For detailed information see Gov.UK "EU legislation and UK law" available at https://www.legislation.gov.uk (date of use: 16 May 2020).

12 Australian Government "Australia - European Union Free Trade Agreement" available at www.dfat.gov.au (date of use: 06 October 2020).

4.2 Organisation for Economic Co-operation and Development

The OECD is a world-wide organisation which replaced the Organisation for European Economic Cooperation, established in 1948 after World War Two.[13] On 30 September 1961, the OECD was officially recognised under the OECD Convention.[14] Membership of the OECD currently stands at 38 countries,[15] while the Council may however; at any time invite a state to join its membership.[16] Over time, the OECD has released various guidelines for its members which bind all members automatically without the need for legislative action unless otherwise agreed.[17]

The OECD considered the inherently international nature of digital networks and computer technologies which challenge the ability of each country to adequately address consumer protection issues in the context of e-commerce and agreed that consumer protection would be better addressed by international consultation and cooperation. Upon this consideration the organisation started working on a set of rules that would protect e-commerce consumers. This work morphed into the Guidelines for Consumer Protection in the Context of Electronic Commerce (the 1999 Guidelines).[18]

Further work on e-commerce and consumer protection led to the enactment of various guidelines and recommendations.[19] Geared towards minimising fragmentation and improving on its work to protect e-commerce consumers, on 24 March 2016 the OECD revised the 1999 Guidelines and replaced it with the OECD (2016) Consumer

13 OECD "About the OECD" available at www.oecd.org/about (date of use: 16 October 2020).
14 Convention on the Organisation for Economic Co-operation and Development, Paris 14 December 1960.
15 See OECD "Partnerships in OECD bodies" for a list of OECD countries available at www.oecd.org (date of use: 03 July 2020); OECD "Where: Global reach" available at www.oecd.org (date of use: 05 September 2020).
16 OECD Convention art 16.
17 OECD Convention art 5.
18 Recommendation of the OECD Council concerning Guidelines for Consumer Protection in the Context of Electronic Commerce 1999 (1999 Guidelines).
19 See for example, the 2006 Anti-Spam Toolkit; the 2007 Mobile Commerce Guidance; the 2008 Online Identity Theft Guidance; 2014 Mobile and Online Payments Guidelines; and the 2014 Digital Content Product Guidelines.

Protection in E-Commerce: OECD Recommendation (CPR). [20] Also related to consumer protection are the Guidelines for Protecting Consumers from Fraudulent and Deceptive Commercial Practices across Borders 2003 (Consumer Protection Guidelines).[21] Both documents are discussed.

4.2.1 Consumer Protection in Electronic Commerce: OECD Recommendation 2016

The CPR was adopted on 24 March 2016 as a revised version of the 1999 Guidelines. The CPR advances the Council's objective of the 1999 Guidelines adopted on 9 December 1999, to limit fraudulent commercial practices through a coordinated global approach by OECD member governments.[22] The 1999 Guidelines were disseminated with the objectives of promoting cross-border trade which benefits both consumers and businesses, by restoring consumer confidence in international transactions; the development of ADR across borders; and the promotion of cooperation among member countries on consumer protection issues.[23]

The success of the 1999 Guidelines notwithstanding, in 2009 a conference was held in Washington District of Columbia (DC) on consumer empowerment.[24] At the conference, the OECD Committee on Consumer Policy (CCP) reviewed basic challenges on the use of mobile devices, unauthorised charges, and poor regulation on acquisition of digital products as well as challenges of misleading and fraudulent commercial practices. Following this review, the 1999 Guidelines were revised. Key new developments in e-commerce addressed by the revised CPR include: the use of fair terms in con-

---

20 OECD (2016) Consumer Protection in E-Commerce: OECD Recommendation, OECD Publishing, Paris.

10 Guidelines for Protecting Consumers from Fraudulent and Deceptive Commercial Practices across Borders 17 June 2003 available at https://www.oecd-ilibrary.org (date of use: 16 September 2020).

22 OECD "Recommendation of the Council concerning Guidelines for Consumer Protection in the Context of Electronic Commerce".

23 Preamble 1999 Guidelines.

24 OECD *Strengthening Consumer Protection*.

sumer transactions;[25] contractual access and information on any limitations on the use of digital products[26] as well as issues on their interoperability.[27] The invasion of data obtained through information collected in exchange of free goods and services is also addressed.[28] The CPR further provides guidance on the treatment of children and vulnerable persons.[29] These developments have broadened the scope of the CPR to include C2C transactions.[30] Through C2C interactions the peer platform market is developed. The OECD policy on peer platform market is that consumers are protected under the general rules governing businesses and consumers.[31]

The CPR, just like the 1999 Guidelines are voluntary guidelines[32] and are self-executing in the sense that they do not require legislation for their implementation. The OECD Council recommends that member states disseminate the CPR to all relevant government and non-governmental institutions.[33]

4.2.1.1 Provisions

The CPR is divided into three parts: Part 1 consists of eight principles on which the work is based; Part 2 sets out implementation procedures, while Part 3 contains recommendations for global cooperation. The CPR applies to B2C transactions and commercial practices which enable C2C transactions.[34] It also covers commercial and non-commercial transactions including transactions that involve products with digital content. B2B transaction does not, however, fall within the purview of the CPR.[35]

---

25 CPR para 6.
26 CPR para 27.
27 CPR para 32.
28 CPR paras 8 and 48.
29 CPR paras 2 and 18; OECD has a mandate to protect children and vulnerable persons who are engaged in e-commerce, see UNCTAD "Consumer protection in e-commerce" 12.
30 CPR Preamble 1.
31 OECD "Protecting consumers in peer platform markets" 7.
32 OECD *Strengthening consumer protection* 4.
33 CPR para 54 (III).
34 UNCTAD "Consumer protection in e-commerce" 2.
35 CPR para 1.

The first principle which is addressed to governments, businesses, consumers, and their representatives provides that "consumers who participate in e-commerce should be afforded transparent and effective consumer protection that is not less than the level of protection afforded in other forms of commerce."[36]

There is the second principle on fair business, advertising and marketing practices which prohibits businesses from making deceptive, misleading, fraudulent or unfair representations or omissions.[37] They may also not promote or market harmful goods or services to consumers and must provide detailed information on their businesses.[38] The CPR has far-reaching provisions on the prohibition of unfair contract terms under this principle. The OECD member states are, in terms of this principle, obliged to adopt legislation to support the use of fair contract terms in consumer contracts.[39] Again, advertisements and marketing communications must be easily identified, and should provide consumers with an opt-out option. Care must be taken in respect of advertisements targeted at children, the elderly, the seriously ill, and other incapacitated persons.[40]

The principle further prohibits businesses from hiding their true identity or location and requires an underlying understanding of jurisdiction and choice of law issues in places where they target consumers.[41] The principle is summarised as follows.

(i) Representations by businesses should be fair, harmless, clear, conspicuous, accurate, accessible, non-deceptive, and should be stored for a reasonable period.[42]

---

36 Ibid.

37 Most of the countries in the OECD have regulations against unfair business advertising. These regulations also apply to online advertising. See OECD *Online advertising trends* 5.

38 CPR paras 4 & 10.

39 CPR para 6, this is similarly provided in the US under the Uniform Computer Information Trans actions Act 2002 which provides for the general application of fair terms and warranties in consumer contracts.

40 CPR para 18.

41 CPR para 21.

42 See OECD *Online advertising trends* 31.

(ii) Businesses must be mindful of regulatory issues affecting different markets.[43]

(iii) Businesses are not to hide their true identity or attempt to circumvent e-commerce regulations.[44]

(iv) Businesses are not to use unfair business terms, especially terms that limit jurisdiction, complaint procedures, or terms which oust the powers of the court. All terms must also be capable of being reviewed or rejected by the consumer.[45]

(v) Commercial communications should be easily known, and consumers should have available options to opt-out of renewable transactions.[46]

(vi) Consumers should not only be capable of confirming their transaction before it is concluded but should also be able to withdraw from a confirmed transaction.[47]

(vii) Special care should be taken in respect of advertisement targeted at children[48] the elderly, seriously ill and other incapacitated or vulnerable persons.

(viii) Businesses should not engage in the collection of consumers' data for deceptive use.[49]

(ix) All terms and conditions with the likelihood of affecting a consumer's decision about a product or service must be made available to the consumer.[50]

---

43 Regulatory issues include the display and sale of banned and recalled products and products without adequate labeling. From 27 to 30 April 2015 the Australian Competition and Consumer Commission inspected products through a sweep operation from 25 countries. This exercise was conducted on behalf of the OECD Working Party on Consumer Product Safety. Of the 1709 products inspected, 693 were banned and recalled products and 880 products were inadequately labeled. See OECD "Online Product Safety" 8-9.

44 CPR para 21; see also OECD *Toolkit for protecting digital consumers* 30.

45 CPR para 6; OECD *Toolkit for protecting digital consumers* 24.

46 OECD "Consumer policy guidance on intangible digital content" 15.

47 OECD *Toolkit for protecting digital consumers* 35; see further CPR para 19.

48 OECD "Consumer policy guidance on intangible digital content" 16.

49 CPR para 8.

50 CPR para 5.

The third principle governs online disclosures and is aimed at providing consumers with as much information as is necessary for them to make informed decisions.[51] It seeks, as far as possible, to make up for the gap in e-commerce where the consumer has no physical opportunity to inspect the item he or she intends to purchase. This is achieved by directing that businesses provide information on price, quality, specification, durability, usage, terms, and conditions online.[52] Disclosure by businesses minimizes the incidence of bait pricing and drip pricing.[53]

The fourth principle governing the confirmation process requires that web-traders must be unequivocal about when and how consumers are to confirm their orders.[54] Transactions should not be processed unless the consumer has access to modify, confirm or withdraw from the transaction.[55] All transactions must be consented to.[56] The tenet behind this provision is to mitigate the effect of errors in e-commerce.

The fifth principle makes provision for secure payment systems. It requires that consumers must be provided with secure payment systems and, where cases of unauthorised or fraudulent charges occur, governments should protect consumers by limiting the liabilities of consumers through the provision of industry-led limitations and chargeback mechanisms for refunds.[57] Measures to counter security and payment-related risks should be implemented by businesses to mitigate the fraudulent "…use of personal data, fraud, and identity theft."[58] Consumers should also have access to retain payment details through storage, printing or e-mails[59] and better procedures for authentication and authorisation are advocated in online payments.[60]

---

51 CPR para 25; OECD *Toolkit for protecting digital consumers* 13, 30.
52 OECD "Improving online disclosures" 2,5; see further CPR paras 31, 32 and 35.
53 These are pricing styles by which products are offered at lower rates and additional charges are gradually introduced as the consumer gets committed to the transaction; see OECD *Toolkit for protecting digital consumers* 26.
54 OECD "Improving online disclosures" 5.
55 OECD *Toolkit for protecting digital consumers* 35.
56 CPR para 38.
57 CPR para 41.
58 CPR para 40.
59 OECD "Consumer policy guidance" 7.
60 UNCTAD "Consumer protection in e-commerce" 7.

The sixth principle governs dispute resolution and redress and its essence is that when things go wrong, the consumer should be reinstated, if not exactly to the position he or she enjoyed before the transaction, at least as close as possible to that position.[61]

The seventh principle provides guidance on privacy and security by recognising that consumers are entitled to enjoy the protection of their privacy as laid down under existing data protection principles.[62] Consumers have rights to fair and lawful processing of their information which should be used for specified purposes only, subject to their agreement and participation and the processing must be minimal and transparent.[63]

Finally, the eighth principle of the CPR details that consumers should be aware of the existence of their rights and how to access them through education. Educating consumers will create knowledge of the existence of these principles and how to access them and, in the process, improve consumers' digital competence.[64]

So as to achieve the objectives of the CPR global co-operation and implementation is highly recommended through self-regulatory practices. In addition, member states are to cooperate in information exchange and other necessary means to combat cross-border fraudulent, misleading, and unfair commercial conducts.[65]

4.2.1.2 Limitations

Principles aimed at consumer protection set out in the CPR compare well with consumer protection principles contained in other regional and international documents. The provisions of the CPR can also be used to fill gaps in some regional

61 OECD *Toolkit for protecting digital consumers* 53.
62 Cate, Cullen, and Mayer-Schonberger *Data protection principles* 15-16.
63 CPR para 48.
64 CPR para 50; see also OECD *Consumer education* 6.
65 CPR paras 53 - 54.

instruments which have not been able to meet international standards within the OECD. There are, however, a few limitations in the CPR.

(a) The CPR was made with a view to complementing existing concepts in consumer protection and in the process, it neglected to delimit its areas of application through definitions. For example, the aim of the CPR as a whole is to protect the consumer but it fails to define who qualifies as a consumer.

(b) The CPR, being a recent regional document, should expectedly provide coverage for technological developments in the fields of e-transferable records and online auctions; this is, however, not the case.

4.2.1.3 Summary

Consumer protection principles as contained in the CPR are in fact a revision of the OECD 1999 Guidelines on Consumer Protection; this revision became a *sine qua non* in view of emerging technologies such as m-commerce. In 2008, the OECD aimed to fill the gap resulting from the use of m-commerce and came up with a policy guideline document[66] which evaluated the concepts and application of m-commerce in detail. Initially, the possibility of applying the 1999 Guidelines on Consumer Protection to the use of mobile gadgets was evaluated. The report however, indicated that adapting the provisions of the 1999 Guidelines to m-commerce would not afford m-commerce consumers the required level of protection. The extant principles in the Guidelines had, therefore, to be expanded to provide for m-commerce-specific challenges.[67]

The CPR, therefore, captures the areas of concern in the use of mobile devices in e-commerce transactions. It resolves issues of software to hardware compatibility, functionality, and inter-operability.[68] The CPR highlights a novel area in consumer transactions where consumers also act as suppliers on some online platforms (C2C

66 OECD *Policy guidance for addressing emerging consumer protection* 2.
67 OECD *Policy guidance for addressing emerging consumer protection* 3-4.
68 UNCTAD “Consumer protection in e-commerce” 3.

transactions).[69] It is now clear that a consumer acting as a supplier must take on all the responsibilities and fulfil all the requirements of a web-trader, for the purposes of that transaction. The CPR also clarifies the use of web agreements and the right of consumers to alter stipulated terms or lay complaints about the unfairness of shrink-wrap or web-wrap agreements.[70] States are further required to ensure unambiguous confirmation processes for consumers,[71] and make provision for an effective dispute resolution process such as ADR or ODR.[72]

Consumer protection for online users under the OECD regime is fairly comprehensive and improvements are required only to address more specific issues such as jurisdiction, the liability of internet intermediaries in relation to consumer transactions, e-transferable records, and online auctions.

4.2.2 Guidelines for Protecting Consumers from Fraudulent and Deceptive Commercial Practices across Borders 2003

The Consumer Protection Guidelines were adopted four years after the 1999 Guidelines on Consumer Protection in E-Commerce which have now been replaced by the CPR. The Consumer Protection Guidelines deal with implementation and are complementary to the recommendations set out in the CPR. The Consumer Protection Guidelines govern the establishment of implementation agencies which provide specifically for the protection of consumers from deceptive cross-border commercial practices. The Guidelines are self-regulatory and were adopted as recommendations

69 One of the paragraphs of the Preamble to the CPR recognises "the dynamic and innovative character of the e-commerce marketplace, which enables consumers to gather, compare, review and share information about goods and services, and fosters the development of new business models, some of which facilitate consumer-to-consumer transactions."

70 CPR para 6; OECD *Toolkit for protecting digital consumers* 24.

71 OECD "Improving online disclosures" 5; OECD *Toolkit for protecting digital consumers* 35; CPR para 38.

72 OECD *Toolkit for protecting digital consumers* 53; CPR paras 43-46.

of the OECD Council on 11 June 2003.[73] According to the recommendation the Consumer Protection Guidelines were formulated:

> recognising that most existing laws and enforcement systems designed to address fraudulent and deceptive commercial practices against consumers, were developed at a time when such practices were predominantly domestic, and that such laws and systems are therefore not always adequate to address the emerging problem of cross-border fraudulent and deceptive commercial practices.[74]

To enforce consumer protection, enforcement agencies must enjoy close co-operation.[75] This is premised on the large number of limitations applicable to the enforcement of consumer protection laws resulting from the actions of cross-border "wrongdoers, victims, other witnesses, documents, and third parties."[76] It is difficult for enforcement agencies to conduct investigations in cross-border activities without inter-state cooperation. Although there are international mechanisms aimed at judicial cooperation and cooperation in the enforcement of criminal law, they may not be effective for cross-border purposes.[77]

4.2.2.1 Provisions

The Consumer Protection Guidelines deal mainly with the enforcement of consumer protection laws among member states and sets out to achieve this through the establishment of enforcement authorities.[78] Fraudulent and deceptive commercial practices are defined in the Consumer Protection Guidelines as practices that occasion harm. The Consumer Protection Guidelines in paragraph I(b) identify such practices to include:

a. Misrepresenting material facts;

b. Failure to deliver goods or services; and

---

73 See recommendation of the OECD Council Concerning Guidelines for Protecting Consumers from Fraudulent and Deceptive Commercial Practices across Borders 2003 (Consumer Protection Guidelines) 3.

74 Preamble Consumer Protection Guidelines.

75 Ibid.

76 Ibid.

77 Preamble Consumer Protection Guidelines.

78 Ibid.

c. Unauthorised debiting; where this would include the practice of charging consumers double fees for services rendered.

Member states are required to cooperate with businesses and private sectors, to further the goals stated in the Consumer Protection Guidelines in order to achieve its goals.[79] To avoid duplication of enforcement actions that could likely occur within the internet space where similar actions could be directed for the same purpose by different enforcement authorities [80] certain measures are proposed. They are notification; information – sharing; assistance with investigation; and confidentiality.[81]

The Consumer Protection Guidelines also provide that member states must keep in good confidence any information which is exchanged in terms of the guidelines.[82] Challenges have been recorded in sharing information across-borders to countries which do not provide strong privacy protection for consumers' personal data.[83] The Consumer Protection Guidelines further recommends a redress system which must be able to provide support and advice. In order to achieve this, member states must jointly study how to attach foreign assets and improve the mutual recognition and enforcement of judgments.[84] OECD member states are finally enjoined to create approaches towards developing additional safeguards against the abuse of payment systems.[85]

79 Consumer Protection Guidelines para 111.
80 Consumer Protection Guidelines para IV.
81 Ibid. Information which are to be shared in accordance with the Guidelines are "publicly available and non-confidential information; consumer complaints; addresses; telephone numbers; net-domain registrations; and basic corporate data; expert opinions and the underlying information and documents on which they are based; third party information; and other evidence obtained in judicial or other compulsory process" see para iv(b) Consumer Protection Guidelines.
82 Consumer Protection Guidelines para IV(f).
83 OECD *Consumer protection enforcement* 6.
84 Consumer Protection Guidelines para VI (4-5).
85 Consumer Protection Guidelines para VI (6).

So far OECD member states have recorded significant progress with cross-border investigation, and this has helped in resolving cross-border fraud cases.[86]

As indicated in the beginning of this chapter, EU member states are influenced by OECD guidelines and regulations but most importantly, they are bounded by EU community laws in the form of Directives and Regulations. Unlike the OECD instruments which do not need to be transposed into national laws, EU community laws are required to be implemented or domesticated into national laws of member states.[87] It is also of note that EU community laws take precedence over national laws of member states.[88] The Directives and Regulations relating to e-commerce in the EU are considered below.

4.3 The European Union

The EU began its journey in 1945 with six founding countries.[89] The aim was to end the incessant wars between neighbours, which had culminated in the Second World War. In 1957, the Treaty of Rome created the European Economic Community (EEC) or Common Market. Through the treaty, member states ceded certain powers to legislate to the EU so creating a trans-national body with its own exclusive powers which existed alongside the concurrent powers of its (at present) 28 member states.[90] To achieve its goals, the EU relies on legislative acts in the form of Regulations,

86 OECD *Report on the implementation of the 2003 OECD Guidelines* 2.

87 Member countries of the EU are to implement laws in commonly agreed areas accord ing to Treaty agreements. The EU Commission therefore only proposes laws in a commonly agreed area, see EU "EU Treaties" available at https://europa.eu (date of use: 16 May 2020).

88 EU "Precedence of European Law" available at www.eur.europa.eu (date of use: 05 June 2020).

89 The European Union was founded by Belgium, France, Germany, Italy, Luxembourg and the Netherlands. See EU "The history of the European Union" available at http://europa.eu (date of use: 21 July 2020).

90 The member states are Austria; Belgium; Bulgaria; Croatia; Cyprus; Czech Republic; Denmark; Estonia; Finland; France; Germany; Greece; Hungary; Ireland; Italy; Latvia; Lithuania; Luxembourg; Malta; The Netherlands; Poland; Portugal; Romania; Slovakia; Slovenia; Spain; Sweden; and the United Kingdom. See http://europa.eu/countries/index (date of use: 21 July 2020).

Decisions, Directives, Recommendations, or Opinions.[91] An EU Regulation is binding and applies throughout the EU member states without further legislative action;[92] while an EU Decision binds only those to whom the decision is addressed.[93] EU Recommendations and Opinions are non-binding guidelines for member states.[94] An EU Directive, on the other hand, is a legislative act that sets out a goal that all EU countries must achieve through implementation in their national laws.[95] A number of Directives and other legislative acts have been adopted by the EU to protect e-commerce consumers. Some provide for consumer protection in specific areas, for example, the Finance Directive provides for consumer protection measures for financial services. However, for consumer protection in respect of distance sales and information-society services, recourse must be had to the following: the Services Directive;[96] the E-commerce Directive;[97] the Unfair Commercial Practices Directive;[98] the Unfair Contract Terms Directive;[99] the Consumer Rights Directive;[100] and the Directive on Consumer ADR.[101] Reference should also be made to the Brussels

91 EU "How the European Union works" available at www.europarliamentti.info.en (date of use: 25 October 2020); see also Giliker (2015) 1 *European Review of Private Law* 8.

92. OECD *Better regulation* 133; see also EU "European Union regulations" available at www.eur-lex.europa (date of use: 25 October 2020).

93 EU "How the European Union works" available at www.europarliamentti.info (date of use: 25 October 2020).

94 Ibid.

95 EU "Regulations, Directives and other Acts" available at https://europa.eu/eu-law/legal-acts (date of use: 16 October 2020).

96 Directive 2006/123/EC of the European Parliament and of the Council of 12 December 2006 on Services in the Internal Market *OJL* 376, 27.12.2006, 36-68.

97 Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on Certain Legal Aspects of Information Society Services, in particular electronic commerce, in the Internal Market *OJL* 178, 17.7.2000 1-16.

98 Directive 2005/29/EC of the European Parliament and of the Council of May 2005 Concerning Unfair Business-to-Consumer Commercial Practices in the Internal Market and Amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council, *OJL* 149, 11.6.2005 22-39.

99 Council Directive 93/13/EEC of 5 April 1993 on Unfair Terms in Consumer Contracts *OJL* 95, 21.4.1993 29-34.

100 Directive 2011/83/EU of the Parliament and of the Council of 25 October 2011 on Consumer Rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council Text with EEA relevance *OJL*, 304, 22.11.2011 64-88.

101 Directive 2013/11/EU of the European Parliament and of the Council of 21 May 2013 on Alterna-

Regulation,[102] and the Rome 1 Regulation[103] as they resolve conflict of law issues within the EU.

Among EU Directives which impacts on online activities of consumers, the E-commerce Directive lays a foundation for the concept of regularisation of e-commerce activities within EU borders.

4.3.1 Electronic Commerce Directive 2000

The E-commerce Directive was adopted in 2000. It was incorporated into national law by most member states in 2002.[104] The Directive is foremost in its rules on commercial communications, e-contracts, and limitations on liability for e-intermediaries.

In the EU activities of service providers are regulated as a "coordinated field". Member states are to regulate these activities within their borders but are not expected to restrict the activities of service providers outside their states or impose registration restrictions on them. [105] This is also premised on the understanding that the establishment of an online company "is not the place where the technology supporting its website is based or accessible, but where it pursues its economic activity."[106]

4.3.1.1 Provisions

The E-commerce Directive is drafted in four chapters, respectively addressing: general provisions; principles; implementation; and final provisions. The E-commerce Directive

tive Dispute Resolution for Consumer Disputes and Amending Regulation (EC) No 2006/2004 and Directive 2009/22/EC *OJL* 165, 18.6.2013 63-79.

102 Council Regulation (EC) No 44/2001 of 22 December 2000 on Jurisdiction and the Recognition and Enforcement of Judgements in Civil and Commercial Matters *OJL* 12, 16.1.2001, 1-23.

103 Regulation (EC) No 593/2008 of the European Parliament and of the Council of 17 June 2008 on the law applicable to contractual obligations *OJL* 177, 4.7.2008 6-16.

104 European Commission, DG Internal Market and Services Unit E2 "Study on the Economic impact of the Electronic Commerce Directive, final report" 7.

105 E-commerce Directive arts 3 & 4.

106 E-commerce Directive recital 19.

basically applies to information society services that include B2B transactions as well as B2C transactions.[107]

Four basic consumer protection measures can be drawn from the E-commerce Directive and they are information requirements;[108] commercial communications;[109] contracts concluded by electronic means; and the limitation of liability of intermediary service providers.

(a) Principle governing contracts concluded by electronic means

This principle validates contracts concluded by electronic means..[110] In terms of this principle, contracts concluded online meets all the requirements of writing, originality, and signature.[111] E-signature is more specifically provided for under the E-signature Directive.[112] Parties are always at liberty to use e-signatures based on individual or organisational arrangements.[113]

The E-commerce Directive further provides a standard for the correction of input errors in respect of contracts with e-robots or AMSs where a consumer places an order through an e-robot or agent. Where an e-robot is used, it is mandatory that the order is immediately acknowledged by the service provider so that the acknowledgement meets the requirements of fixation and reproduction. The acknowledgement will not take effect until the consumer has accessed it.[114] This additional safeguard protects

107 Examples of information society services include the online sale of goods, entertainment, advertising, information services, professional services; intermediary services but exclude the delivery of goods. Some of these services are provided without cost to the consumer although they could be funded privately or by advertisement, see the E-commerce Directive recital 18 and 21.

108 E-commerce Directive art 1(5).

109 E-commerce Directive arts 6-8

110 E-commerce Directive art 9. The Directive deals with the forms an e-contract should be presented and not the substantive nature or content of the contract itself. National laws validating the substance of a contract applies to e-contracts.

111 Lindholm and Maennel “Directive on Electronic Commerce” (2000/31/ec)” 21-22.

112 Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures. In arts 1& 2 the Directive provides “for the facilitation and recognition of the use of e-signatures and advanced e-signatures”.

113 E-signatures Directive recital 16.

114 E-commerce Directive art 11(1).

consumers from being bound by contracts entered into automatically without an opportunity to review the contract. The stringent requirement of an acknowledgement is however, dispensed with in transactions made directly with consumers without the use of an AMS.[115] In the latter case, consumers should nevertheless be provided with means to correct input errors, where necessary before a transaction is concluded. In the event of a dispute between parties, the Directive provides for out-of-court settlement which could be in physical space or by electronic means.[116]

(b) Principle governing information requirements

Service providers should make available certain information to consumers before transactions are validated.[117] The information requirement is compulsory and cannot be waived in a consumer contract.[118] For instance, a service provider should indicate any relevant code to which he or she has subscribed and how to access the code. The relevance of codes of subscription to those who have subscribed is that they are under a duty to keep to the dictates of such codes.[119]

115 E-commerce Directive art 11(2).

116 E-commerce Directive art 17.

117 E-commerce Directive art 10.

118 In *Bundesverband der Verbraucherzentralen und Verbraucherverbande – Ver braucherzentrale Bundesverband eV(Federal Union) v Deutsche Apotheker- und Arztebank eG* (*DAAB*) C-380/19 (judgement of the Court – sixth chamber was delivered on 25 June 2020) the court combined the provisions of art 13 of the ADR Directive and art 6(1)(t) of the CRD to hold that information must not only be given to consumers but must be given "in good time before the contract is concluded" see para 33. The *DAAB* operates a website for its banking business but does not conclude contracts on that site see para 10. On its site it provides legal notice on ADR and there is a tab on the site with a downloadable version of its terms and conditions. Those terms and conditions, however, do not contain the willingness of *DAAB* to participate in a dispute resolution process. The contention of the *Federal Union* is that the terms and conditions of *DAAB* should reflect their willingness to participate in a dispute resolution process before a consumer conciliation body (para 12). The court ruled that submission to a dispute resolution process must be provided in the general terms and conditions; that "it is not sufficient in that respect that the trader either provides that information in other documents accessible on his website, or under other tabs thereof…" (para 37).

119 Hathaway and Savage "Duties for internet service providers" 4. Furthermore, through subscription to private or professional codes service providers could be sanctioned and prevented from participating in professional activities. Such far-reaching consequences are a deterrent to misconduct. See also Educaloi "Rights and responsibilities of service providers in contracts for services" available at https://www.educaloi.qc.ca (date of use: 16 October 2020).

Service providers are required to stipulate the technical steps which consumers are to follow.[120] This information should also include the language of the contract. Under this provision there is room for consumers to correct input errors before confirming their orders.[121] Consumers are protected from hidden contract terms as all terms should be available to consumers conspicuously, and should be capable of beign reproduced and stored.[122] It is evident that where service providers are in breach of any of the measures provided under this principle, the contract can be voided at the instance of the consumer.[123]

(c) Principle governing commercial communications

Commercial communications referred to here are essentially advertisements, and although the E-commerce Directive does not prohibit advertisements, they are subject to its regulations. The E-commerce Directive provides that commercial communications should be easily ascertained with clear indication of their source. Where the communication involves promotional offers, competitions, or games which entitle consumers to discounts, premiums, or gifts, the conditions for qualification and participation must be clear and should be subject to compliance with the professional rules and conduct of regulated professionals.[124] Member states are furthermore required to ensure that service providers engaged in the distribution of unsolicited mails or spam[125] provide access to open opt-out registers in which consumers not wishing to receive such mails, may register.[126]

(d) Principle governing limited liability of internet intermediaries

Service providers are not liable for activities which are merely technical, for instance where they are acting as a mere transmitter or conduit.[127] To qualify as a mere conduit,

120 E-commerce Directive art 10(1)(a).
121 E-commerce Directive art 10(1)(c).
122 E-commerce Directive art 10(3).
123 Vagadia “Contract discharge and methods to reduce liability” 74.
124 E-commerce Directive arts 6 & 8.
125 Spam is discussed in chapter 2 para 2.6.3.8.
126 E-commerce Directive art 7.
127 E-commerce Directive recital 42; see also Baistrocchi (2002) 19/3 *Computer & High Technology*

a service provider transmitting information should not initiate or modify the information they transmit and neither should they select the recipients.[128] And where the service provider does not modify the information transmitted, he or she will "not be liable for the automatic, intermediate, and temporary storage of that information."[129]

While the E-commerce Directive provides for limited liability for intermediaries who offer only conduit, caching, and hosting services, certain member states have included in their national provisions, limited liability for other intermediaries who make available hyperlinks and search engines that provide links to information sources.[130]

Notwithstanding, an ISP will be held liable where it becomes aware of infringing content and does nothing to remove it.[131] Where there are cases of infringement or a likelihood of infringement, the court or an administrative body may issue injunctions on the ISP to remove the infringing content or disable access to it. The ISP may also be ordered to disclose the identity of third parties. With respect to cases on infringement on the website, courts have granted injunctions restraining access to such a website.[132] However, there is a need for harmonised rules and procedures on how to prevent or eliminate infringing content on websites.[133] A harmonised procedure would undoubtedly be preferable as available options for take down notices could include notices from individuals,[134] or possibly an application to court. Conceding that it may

---

Law Journal 118.

128 Adeyemi (2018) 24/1 *Computer and Telecommunications Law Review* 9.

129 E-commerce Directive arts 12-13.

130 Dinwoodie ed *Secondary liability* 5-7.

131 See the cases of *Sir Elton John & ors v Countess Joulebine* (2001) MCLR 91; *Godfrey v De mon Internet Ltd* (1999) QBD 26; see also Verbiest *et al*, *Study on the Liability of Internet Intermediaries* 1-3.

158 E-commerce Directive art 15(2); see also *Totalise v Motley Fool Ltd* (2001) All ER (D) 290 (Dec)*; Grant v Google* (2006) All ER (D) 243 (May); for more cases where the courts granted injunctions restraining access to websites with infringing materials see the cases of *Religious Technology Center v Netcom On-line Communications Services, Inc* 907 F Supp 1361 (Dist Court ND California 1995-Google Scholar) 1382-1383 and *A&M Records, Inc v Napster, Inc* 239 F 3d 1004 (Court of Appeals, Ninth Circuit 2001) 1011.

133 E-commerce Directive art 15, currently, there are disparate rules governing take-down notices in different national laws within the EU as there are no specific procedures for take down notices in the Directive. Service providers are only required to inform appropriate authorities of any known or likely infringement.

134 See for instance s 77 of the ECTA.

be safer for ISPs to act only on court orders in order to prevent an abuse of the process and possible cases of liability to their subscribers, relying only on court processes may frustrate a quick action in the case of a clear case of infringement. It is would appear that the issuance of take-down notices by Tribunals within limited time frames pending investigation, would better serve the purpose.[135]

Finally, ISPs should not be compelled or bound to account for the information they transmit provided they act as mere conduits.[136] This implies that ISPs are not expected to play other roles besides fulfilling technical functions, if they are to benefit from non-liability for infringing content or materials. This requirement is based on the impracticalities which may arise if ISPs are compelled to monitor the millions of websites to which they provide access. Furthermore, such a task may lead to very stringent conditions for use of the website by third parties and the cost of accessing the websites may become prohibitive.[137] While issues emanating from liabilities of ISPs in online content might seem far-fetched in consumer contracts, it is indeed relevant as consumer contracts are influenced by information on the internet. Sometimes the information could be wrong, fraudulent, or misleading and could cause loss and damages.[138]

Article 21 forms part of the concluding provisions of the E-commerce Directive; the article provides that in 2003, and every two years thereafter, the Commission must submit a detailed report on the application of the Directive to the EU Parliament and Council. Pursuant to the objectives of article 21, the first report of the Commission on the application of the E-commerce Directive was submitted to the European

135 For a detailed discussion on the intricacies and procedures for take-down notices see Urban, Karaganis and Schofield (2017) 64/3 *Journal of the Copyright Society of the USA* 384-388.

136 Biastrocchi (2003) 19/1 *Computer and High Technology Law Journal* 126.

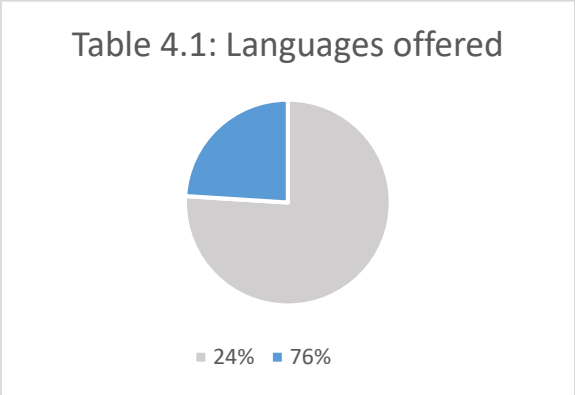
137 See E-commerce Directive recital 47; see also Riordan *The Liability of Internet Intermediaries* 19.

138 In *Schnabel v Trilegiant Corp* 697 F3d 110 (2012) 112ff the Plaintiffs claimed that they were misled into a contract with a post transaction third party who billed them monthly. The information on the website did not indicate clearly that the Plaintiffs will be on monthly subscriptions without their consent, thus the action in court.

Parliament in 2003.[139] In the report, the Commission acknowledged that growth in the use of the internet in EU households had increased from eighteen per cent in 2000 to 43 per cent in 2002.[140] It evaluated adherence by member states to the national incorporation time-table, and concluded that only three states – France, the Netherlands and Portugal – were yet to comply at the time of the report.[141] In examining the benefits of the Directive, the Commission considered whether websites complied with information requirements as provided for in the Directive. This was done through studies carried out by a German Association of Consumers and by European Consumer Centers.[142]

The infographic of some of the European Consumer Centers' studies carried out between October 2002 and February 2003 are represented below.

Table 4.1 Languages offered



Grey (76%) represents websites with no language options
Blue (24%) represents websites that offered different languages.
Of the 24% that offered different languages, 62% offered 2 languages, 22% offered 3 languages, 10% offered 4 languages and 6% offered 5 languages.
Courtesy: European Consumer Centers

Courtesy: VZBV (Verbraucherzentrale Bundesverband - German association of consumer organisations) 2003

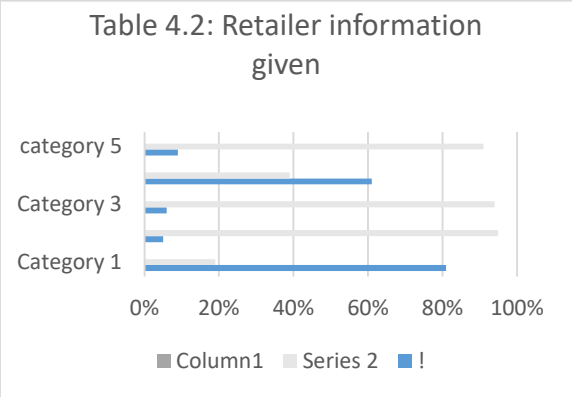
139 Report of the Commission to the European Parliament, the Council and the European Economic and Social Committee "First Report on the Application of Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on Certain Legal Aspects of Information Society Services, in particular Electronic Commerce, in the Internal Market" ("First report on application of Directive on Electronic Commerce") 2003.

140 "First report on application of Directive on Electronic Commerce" 4.

141 "First report on application of Directive on Electronic Commerce" 6.

142 There was a sampling of websites by VZBV (Verbraucherzentrale Bundesverband-German association of consumer organisations) see Report from the Commission to the European Parliament the Council and the European Economic and Social Committee see "First report on application of Directive on Electronic Commerce" 9.

Table 4.2 Retailer information given



Grey represents 'No' (Information is not on the website)

Blue represents 'Yes' (information is on the Web-site)

Category 5 –Address of Retailer
Category 4- Registration Number
Category 3- Phone Number of Retailer
Category 2- E-mail Address
Category 1- Contact Name
Courtesy: European Consumer Centers

Courtesy: VZBV (Verbraucherzentrale Bundesverband - German association of consumer organisations) 2003

From Tables 4.1 and 4.2 above it is clear that websites fell short of the requirements laid out in the E-commerce Directive as it relates to the provision of information to consumers. From Table 4.2 above, consumers had little or no access to the e-mail addresses or phone numbers of online retailers. This clearly shows the nature of impediments which consumers face online. In response, the Commission indicated in its report that most ISPs were unaware of the information requirements, but on being informed, they started to comply.[143]

4.3.1.1 Exclusions

The E-commerce Directive does not apply to individual communications or personal contracts whether by e-mail or other means; or simply put, C2C communications.[144] It does not apply to: taxation; the provision of offline services; data protection; [145]

143 "First report on application of Directive on Electronic Commerce" 9.

144 E-commerce Directive recital 18.

145 Data protection is addressed in a good number of Directives and Regulations in the EU. These include: Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (this Regulation repeals Directive 95/46/EC of the European Parliament and is referred to as the General data protection regulation-GDPR); Directive

gambling activities;[146] employment relationships; non-electronic activities such as auditing; litigation; notarization; agreements on cartel law; and medical advice which is of a non-general nature.[147]

As regards contracts, the following are excluded from the provisions of the E-commerce Directive:[148]

(i) Contracts that create or transfer rights in real estate, except for rental rights.
(ii) Contracts requiring by law the involvement of courts, public authorities or professions exercising public authority.
(iii) Contracts of suretyship and collateral securities by consumers.
(iv) Contracts governed by family law or the law of succession such as wills.

The restrictions on the application of the E-commerce Directive to certain contracts which have been referred to above are not absolute in that member states may permit certain exclusions. Member states are, however, required to submit their decisions to the Commission every five years.[149]

4.3.1.2 Limitations

A critical analysis of the principles underlying the protection of e-commerce consumers in the EU as contained in the E-commerce Directive, does not address the time and place of receipt and dispatch of messages in e-transactions, and this needs to be

97/66/EC of the European Parliament on the Processing of Personal Data and the Protection of Privacy in the Telecommunications Sector; 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 Communication Sector which is soon to be repealed by the proposed Regulation on the respect for private life and the protection of personal data in electronic communications (ePrivacy Regulation).

146 The exclusion of gambling activities does not include promotional competitions or games where The purpose is to encourage the sale of goods or services and where payments are only meant to secure the promoted goods or services.

147 E-commerce Directive art 1(5).

148 E-commerce Directive art 9.

149 E-commerce Directive art 9(3).

clarified. In e-commerce conventional rules on time and place of contract may not be appropriate for all aspects of e-contracting.[150]

Article eleven of the E-commerce Directive merely refers to acknowledgment of receipt from the service provider where an order has been placed. This article does not prohibit failure to acknowledge an order unlike the provisions of the UNCITRAL Model Law in its article 14, wherein there is a consequence for non-acknowledgement. The article provides that where a data message (in this case, an order) is not acknowledged within agreed time frames the obligation between the parties is effectively terminated. Nonetheless, an overall appraisal of the EU regulatory framework shows a significant level e-commerce consumer protection. Furthermore, salient principles on e-contracting as enshrined in the UNCITRAL Model Law and the EC Convention are properly captured and expanded in the EU Directives on E-commerce. These principles are also soundly implemented by the different consumer protection centers and other implementation agencies within the EU.

The crux of the matter, however, is that although there is some measure of protection for e-commerce consumers in the EU, that level of protection is restricted to trade within EU member states. This presupposes that European consumers doing business with suppliers outside of the EU may not enjoy the same level of protection available if they do business with suppliers within the EU region. They will also have to face the problem of differing consumer protection laws outside of the EU.

150 It should be noted that the concept of “place” in an e-contract has been unequivocally clarified in article 15 of the UNCITRAL Model Law and article 6(4) of the EC Convention, which provides that a place is not restricted to the location of an information system, but also to where the parties are physically located. This principle has been included in various regional and national laws thus giving it credence as an international standard. See similar provisions in s 15 Uniform Electronic Transactions Act 2002 (UETA); ss 12-14 SADC Model Law; s 13 Electronic Communications and Transactions Act 25 of 2002 (ECTA); and s 14A Electronic Transactions Act 162 of 1999 (ETA). The position is slightly different in most African regions where the determination of receipt is subject to acknowledgement of receipt; see art 22 of the AU Convention, 2014; art 21 of the ECOWAS supplementary Act, 2010; and s 28 of the Electronic Transactions Bill, 2017.

4.3.2 Consumer Rights Directive 2011

The CRD was preceded by Directive 97/7/EC on the Protection of Consumers in respect of Distance Contracts (CPD). The CPD made provision for both distance contracts and e-contracts. In 2008, due to issues emerging in e-commerce and consumer protection, the EU introduced proposals for a new Directive that would be more comprehensive.[151] The Directive on Consumer Protection in respect of Contracts Negotiated away from Business Premises [152] and the Directive on Consumer Protection in respect of Distance Contracts were reviewed to close unwanted gaps and remove inconsistencies.[153] It was during the review process that it was considered appropriate to replace the two Directives with a single Directive. [154] By 2011, the CRD[155] had been adopted and proposed for incorporation into national laws of all member states as the new Directive for the protection of consumers' rights.[156] The CRD was further amended in 2019 to better the enforcement and modernisation of the CRD. It was also amended to create rules for C2C transactions, expand the scope of application to cover both commercial and non-commercial activities and give details of penalties for offences committed in the CRD, amongst other amendments.[157] Article 5 of the Directive on Better Enforcement and Modernisation also creates access to online dispute resolution.[158]

---

151 Lilleholt (2009) 17/3 *European Review of Private Law* 335.

152 Council Directive 85/5777/EEC to protect the consumer in respect of contracts negotiated away from business premises.

153 Radic (2013/2014) *European Consumer Law* 2.

154 See recital 2 CRD.

155 2011/83/EC of 25 October 2011 on Consumer Rights, amending Council Directive 93/13/EEC (on Unfair Terms in Consumer Contracts) and Directive 1999/44/EC of the European Parliament and of the Council (Directive on Certain Aspects of the Sale of Consumer Goods and Associated Guarantees), and repealing Council Directive 85/577/EEC (on Protection of Consumers in respect of Contracts Negotiated away from Business Premises) and Directive 97/7/EC of the European Parliament and of the Council (Directive on the Protection of Consumers in respect of Distance Contracts).

156 The CRD was incorporated into national laws of member states by December 2013 with effect from 13 June 2014, see art 24 CRD.

157 The CRD is amended by Directive (EU) 2019/2161 of the European Parliament and of the Council of 27 November 2019 amending Council Directive 93/13/EEC and Directives 98/6/EC, 2005/29/EC and 2011/83/EU of the European Parliament and of the Council as Regards the Better Enforcement and Modernisation of Union Consumer Protection Rules *OJL* 328, 18.12.2019 p 7-28 (Directive on Better Enforcement and Modernisation).

158 Consumers are encouraged to access ODR through Regulation (EU) No 524/2013 of the Euro-

4.3.2.1 Provisions

The CRD applies to three categories of contract: distance contracts; off-premises contracts; and other contracts which are basically on-premises contracts. The CRD has five chapters. In Chapter 1 the scope of the Directive is set out and this chapter includes the definition of terms. Chapter 2 provides for information requirements which businesses must fulfil for the conclusion of on-premises consumer contracts. This chapter does not apply to e-commerce consumers and will therefore not be discussed. Chapter 3 contains the information requirements for distance and off-premises contracts and also regulates the right of withdrawal.[159] Chapter 4 details the rules governing delivery and the passing of risk applicable to contracts for the sale of goods, and further sets out rules for all types of consumer contracts; while Chapter 5 of the CRD, deals with enforcement and penalties.

The CRD aims at harmonising certain aspects of consumer contracts within the European Community and to that extent, member states may not maintain or introduce divergent provisions in their national laws.[160] The requirement of full harmonisation in the CRD is questioned as some opinions favour a minimum approach or commercial code as they argue that a Directive ought not to follow a full harmonisation approach.[161] Nonetheless, the provisions of the CRD are imperative and national laws are not permitted to waive or restrict any of the rights it contains, and if they do so, the inconsistent provisions will be of no effect.[162] The CRD therefore, applies a fully

pean Parliament and of the Council of 21 May 2013 on Online Dispute Resolution for Consumer Disputes and amending Regulation (EC) No 2006/2004 and Directive 2009/22/EC (Regulation on Consumer ODR).

159 CRD arts 6, 8-16.

160 CRD art 4. Minimum approach is argued by author Giliker that although it allows member states to impose more stringent measures that are consistent with a particular Directive it however, leads to fragmentation and diversity in national laws, see Giliker (2017) 37(1) *Legal studies* 79.

161 Chirita "The impact of Directive 2011/83/EU on consumer rights" 17 & 27.

162 CRD art 25.

harmonised framework geared towards eliminating the difficulties which consumers faced under the CPD.[163]

The minimum harmonisation clauses in the CPD led to legal fragmentation and an unequal level of consumer protection across the EU.[164] Following efforts at harmonisation, the 2017 impact assessment report on the CRD shows that consumers are better protected in the EU in view of the unified framework as regards both regulation and enforcement.[165] The level of harmonisation within the EU provides greater protection for consumers compared with other regions where there are divergent laws on e-commerce. The CRD does not, however, harmonise language requirements applicable to consumers,[166] neither does it regulate general contract laws. These unregulated aspects are to be dealt with by member states according to their national laws.[167]

The CRD applies to contracts between businesses and consumers and between consumers.[168] A consumer is defined as:

> a natural person acting outside of his or her trade or profession…where a contract is concluded for dual purposes, partly within and partly outside of the person's trade, and the trade purpose is insignificant, that person should be regarded as a consumer.[169]

The definition of distance contracts includes, but is not limited to, e-contracts and further includes other means of contracting, such as through mail orders.[170] The CRD applies to the transport of goods and car rental services subject to the qualification that

163 European Parliament *Towards new rules* 28; Howels & Reich "The current limits of European harmonisation" 52.

164 Commission of the European Communities, Commission Staff Document Accompanying document to the proposal for a Directive on consumer rights. Executive summary of the impact assessment 2008 at 3.

165 European Commission, Commission Staff Working Document Evaluation of the Consumer Rights Directive 2017 20.

166 CRD recital 15.

167 See CRD recital 14, arts 3(5) & 6(7); see further Manko "Contracts for supply of digital content" 4.

168 CRD art 1, art 1 of the CRD was expanded in para 27 of the Directive on Better Enforce ment and Modernisation to regulate contracts between consumers. It provides that online market platforms are to disclose the status of third party traders so that consumers will know whether they are trading with traders or consumer as themselves. Transactions between consumers are not protected in terms of consumer protection regulations; see further art 6(a) (b)-(c) of the Directive on Better Enforcement and Modernisation.

169 CRD recital 17.

170 CRD recital 20.

the right of withdrawal does not apply to the latter types of transactions.[171] It also applies to auctions using on-line platforms.[172]

The CRD regulates the nature of information which suppliers must provide; withdrawal rights; delivery and payment methods as well as inertia selling as discussed below.

(a) Information requirements

Consumers are protected online through the quality of information which the CRD requires of suppliers.[173] In order to meet the requirements of the CRD, businesses are mandated to clearly provide information on their goods and their businesses on a durable medium,[174] which in the case of e-commerce could be on e-mails or websites. The website must, however, be capable of retaining the information and should be accessible to the consumer for future reference.[175]

The CRD makes provision which covers m-commerce transactions through rules on the use of devices with limited space or single window facility.[176] It provides that when such media (devices with limited space) are used, the trader shall provide, on that

171 CRD recital 27.

172 CRD recital 24.

173 Information which are to be provided should refer to goods and their qualities, total price inclusive of taxes, additional freight, delivery, the cost of communication if not charged at a regular rate and other applicable costs see CRD art (6)(e). In terms of art 8(1) of the CRD in addition to information on goods, suppliers are required to provide information on the business. This information should include information on the supplier's identity and trading name on a durable medium which could include appropriate websites and other durable means of e-communications, arts 8(1) & 6(1) provides further elaboration on information which suppliers are to provide.

174 Durable medium is defined in art 2(10) of the CRD as "any instrument which enables the consumer or trader to store information addressed personally to him in a way accessible for future reference…" and recital 23 of the CRD give examples of durable media to include "paper, USB sticks, CD-ROMS, DVDs, memory cards, or the hard disks of computers as well as e-mails."

175 See the case of *Content Services Ltd v Bundesarbeitskammer* (2012) Case C-49/11; where in para 47 of the judgement of the 3rd Chamber on preliminary issues brought before it, the Court referred to a 2007 report of the European Securities Markets Expert Group (ESME) which classified websites into ordinary or sophisticated websites and noted that sophisticated websites could serve as durable media. In para 48 of the same judgement, Content Services Ltd explained that with new technologies some websites could enable the retention and reproduction of information over a period of time for the use of consumers. The Court in para 50 held that a website which could not achieve retention and future reproduction without alteration could not constitute a durable medium. supplier's information should contain geographical location of the business office, phone number and other related contact information, art

176 Issues on limited space could arise from contracts concluded through SMS see EU DG Justice *DG Justice guidance document concerning Dir 2011/83/EU* 33.

particular medium, the required information in a way appropriate to the means of communication.[177] In my opinion, if there are links to a website with more detailed texts, the link should be provided and, if possible, the contract may be concluded through that link. This will ensure that the consumer actually visits the link. Information on the interoperability of software and devices and the functionality of digital contents must also be made available to consumers.[178] Furthermore, the information requirement should address problems associated with over consumption and misleading advertisements especially for digital products targeted at minors.

(b) Withdrawal rights

The right to withdraw from a contract is recognised in the CRD and information on this right must be unequivocally presented to a consumer in an online transaction.[179] Of course, this right will not avail consumers whose transactions are not capable of being withdrawn under the provisions of the CRD, the display of the withdrawal information notwithstanding.[180]

177 CRD art 8 (4).

178 see CRD art 6 (r) and (s).

179 See art 6(16) of the CRD. This right can be exercised within fourteen days of entering into a contract with or without reasons CRD art 9; see further European Parliament *Towards new rules* 7. In accordance with art 10(1) of the CRD this period may, however, extend by a twelve-month period where the trader does not meet the requirement of the CRD which mandates traders to inform consumers of their right to withdraw. However, the withdrawal period reverts to fourteen days immediately the trader informs the consumer of his or her right to withdraw at any time during the twelve-month period, see art 10(2).

180 Article 16 of the CRD lists out some transactions which do not entitle consumers to the exercise of the right of withdrawal and they include contract for services that has been fully performed, or for digital content which is not supplied on a tangible medium where the performance of the service began with the consumer's express consent and acknowledgment that he or she would lose his or her right of withdrawal once the contract had been fully performed by the trader. (It is worth noting that mere knowledge by the consumer that he or she will lose his or her right of withdrawal is not enough, there must be an express acknowledgement to that effect). Other contracts in this category includes the supply of goods or services which fluctuates; contracts where the goods were made to the consumer's specifications or personalised; contracts in respect of goods that can deteriorate or expire rapidly and contracts for the supply of sealed goods which may become unhealthy after it has become unsealed. Others are contracts for the supply of goods which by their nature mix inseparably with other items; the supply of alcoholic beverages, the price of which was agreed to at the time of the conclusion of the sales agreement, the delivery of which can only take place after 30 days, and the actual value of which is dependent on fluctuations in the market which cannot be controlled by the trader. Contracts for the supply of sealed audio or video recordings or computer software which have been unsealed after delivery; the supply of newspapers, periodicals, or magazines, with the exception of subscription contracts for the supply of such publications; contracts at public auction as well as con-

For a withdrawal process to enjoy validity, the consumer must inform the trader of his or her decision to withdraw from the contract within the withdrawal period using the model withdrawal form which is annexed to the CRD, or by making an unequivocal statement setting out the decision to withdraw from the contract. The onus is on the consumer to show that the procedure for withdrawal was properly followed.[181] In withdrawing from a contract or sales agreement, a consumer shall not bear any costs other than the direct cost of returning the goods. However, a consumer would not bear the cost of returning the goods if the trader has agreed to bear that cost or failed to inform the consumer that he or she must bear the cost of returning the goods.[182]

In all events, when the right of withdrawal is properly exercised the trader shall, within fourteen days of being informed by the consumer of his or her decision to withdraw from the contract, or of receiving the goods or evidence that the goods have been sent in a sales contract, whichever applies, reimburse all payments received from the consumer using the same means of payment used by the consumer, or any other means provided by the consumer.[183] Where a consumer has withdrawn from such contracts, all connected contracts shall be terminated automatically.[184]

(c) Delivery and fee payment methods

Unlike some earlier regulations on consumer protection, the delivery of goods is regulated in the CRD. There are time-specific to protect consumers against late or no

tracts for the provision of accommodation outside residential use and related leisure activities. The above exclusions listed in art 16 of the CRD have been expanded to include the delivery of non-network energy as a result of fluctuations, this is provided in para 43 of the Directive on Better Enforcement and Modernisation.

181 CRD art 11(4); for an insight into the necessity for withdrawal within the stipulated withdrawal period, see the case of *Travel Vac SL v Manuel Jose Antelm* Case C-423/97, (1999) ECR p1-2195 at paras 49 & 51; on a discussion of the case see Loos "Right of withdrawal-Interoperability of Directives" 545-547.

182 CRD art 14 (1). A consumer will also not bear any costs if the trader fails to provide him or her with a confirmation of the concluded contract on a durable medium within a reasonable time after the contract has been concluded, or at the time of the delivery of the goods, or before the performance of the service begins see CRD art 8(7).

183 CRD art 13.

184 CRD art 15.

delivery after the conclusion of a contract. Articles 18-19 provide that where a consumer is unable to access the goods within 30 days, or some other agreed duration after placing an order, the consumer shall notify the trader and set out an additional time frame within which the goods may be delivered. The provision for additional time for performance will only apply if there was no fixed agreement on a delivery time between the trader and the consumer due to the nature or use of the goods. In any event, should the trader fail to deliver the goods by the expiry of the extended period, the consumer may terminate the contract immediately and is entitled to reimbursement.[185] Furthermore, the trader bears any risk of loss of or damage to goods until delivery save where the mode of transportation of the goods was at the consumer's sole discretion.[186]

In the CRD, consumers may not be charged any amount by the trader, exceeding the amount the trader pays for the use of any payment system or telephone charges.[187] If there are additional charges, the consumer will not be bound by the contract except he or she consents. Additional charges will result in the consumer acquiring a right to reimbursement of such charges, any default rules notwithstanding.[188]

(d) Inertia selling

As part of marketing drives, retailers go the extreme lengths to deliver unrequested products to unsuspecting consumers, either as promotional sales or as samples. This practice is widespread and is referred to as inertia selling. Inertia selling is the act of sending unrequested goods to householders followed by a bill for the price of the goods if they do not return them.[189] It has the effect of compelling consumers to pay for goods which they ordinarily might not have purchased, and is, therefore, an unfair market practice. Under the CRD, inertia selling is prohibited. Where there is an

185 European Parliament "Towards new rules" 7.
186 CRD art 20.
187 See arts 19 and 21 of the CRD, both articles form part of the improvement of the CRD on the previous Consumer Protection Directive.
188 CRD art 22.
189 *Collins English Dictionary* available at www.collinsdictionary.com (date of use: 25 October 2020).

unsolicited supply of goods, digital content, or services, consumers are exempted from making payments.[190] Inertia selling is also listed under item 29 of Annex 1 of the Unfair Commercial Practices Directive[191] as an unfair commercial practice.

Compliance with the provisions of the CRD is the responsibility of public bodies or their representatives, as well as legitimate consumer and professional organisations.[192] Compliance must be backed up by penalties for the infringement of national laws as it relates to the CRD. These penalties must be effective and should dissuade non-compliance.[193] Member states must inform consumers and other stakeholders of their rights under the CRD.[194] Every EU member state must have a European Consumer Centre where consumers can easily lodge complaints.[195] For the purposes of effective monitoring, the Commission was required to submit a report to the European Parliament on the application of the CRD, supported by legislative proposals where necessary, by 13 December 2016.[196]

4.3.2.2 Exclusions

Article 3 provides that the CRD shall not apply to contracts on the creation or transfer of immovable properties;[197] transport services in relation to passenger transport; social services; supply of consumables; and contracts for the single use of an internet

190 CRD art 27.

191 Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concern ing unfair Business-to-Consumer commercial practices in the internal market *OJL* 149,11.6.2005 22-39.

192 Cauffman (2012) 19/1 *Maastricht Journal of European and Comparative Law* 217.

193 CRD arts 23-24.

194 CRD art 26.

195 EU "Role of the ECC-NET" available at www.ec.europa.eu/cpc (date of use: 02 October 2019).

196 CRD art 30. This report was indeed made available on the 23 May 2017 entitled "Report from the Commission to the European Parliament and the Council on the Application of Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on Consumer Rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Par-liament and of the Council and Repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council" available at https://eur-lex.europa.eu (date of use: 20 October 2020).

197 On immovable properties see Cauffman (2012) 19/1 *Maastricht Journal of European and Com parative Law* 213-214.

connection. The right to withdraw from a contact as contained in article 9 of the CRD is inapplicable in respect of personalised goods or services and also inapplicable to perishable goods or goods which are subject to price fluctuations.[198]

4.3.2.3 Limitations

The CRD specifically provides for rights of consumers while trading online, by distance, and off-premises. These provisions have far-reaching effects and are wider than previous regulations on the protection of e-commerce consumers in the EU. However, there is still an urgent need to address legal issues that are specifically posed by the application of m-commerce. These issues include the online protection of minors and over-consumption of m-commerce by minors as a result of commercial exploitation.

There is a further need for suppliers or providers to give additional information to users of digital content. Most software comes with regional coding or other geographic restrictions, copy limitations, use expiration and inoperability issues. The information on use limitations is not always made available to consumers upfront and could be inconvenient. The CRD focuses mainly on resolving challenges associated with interoperability but does not deal concisely with these other issues.[199]

With improved legislation and provision for effective implementation, it is trite that consumers are educated on the existence of their rights and the ease of enforcement. There is a need for massive education on consumer rights and the creation of available options for dispute resolution in each country. The dearth of consumer awareness as regards their rights has limited the use of e-commerce activities, especially in cross-border trade. According to Eurobarometer,[200] in 2001 the major

198 CRD art 16.

199 Jacquemin (2017) 8 *JIPITEC* 31.

200 Commission of the European Communities "Consumer Behaviour in the Internal Market" July 1991 at 17 available at http://www.ec.europa.eu/public_opinion/archives/eb_special.htm (date of use: 02 October 2020).

impediments to cross-border trade, were identified as follows: 30 per cent of Europeans felt that it was too difficult to exchange a product or have it repaired; sixteen per cent felt that dispute resolution was difficult; fifteen per cent had issues with obtaining information and advice; fourteen per cent were uncertain about sale conditions; ten per cent were uncertain about safety standards; nine per cent were uncertain about quality standards; while seven per cent complained of difficulties in making payments. In all, 87 per cent of Europeans had complaints.

Still on constraints faced by consumers online, a more recent study shifted consumers' fear to the level of protection which will be available to consumers in respect of transactions with businesses which are established and located outside the EU and the possibility of extraterritorial enforcement.[201]

4.3.3 Jurisdiction in the European Union

Given Europe's unified legal system, jurisdiction does not present a problem in that recourse is had to the Council Regulation on Jurisdiction, the Recognition and Enforcement of Judgments in Civil and Commercial Matters Regulation[202] (the Brussels Regulation), and the Rome 1 Regulation on the Law Applicable to Contractual Obligations[203] (the Rome 1 Regulation) together with the rulings of the European Court in dispensing justice under the European legal system.

There are indications in the E-commerce Directive of the law applicable to consumer contracts through references to the country-of-origin principle and the principle governing the place of establishment.[204] Jurisdiction in the EU is largely governed by the application of the Brussels Regulations[205] and it enjoys application across EU

201 Muller *et al Consumer behaviour* 23.
202 Council Regulation (EC) 44/2001 of 22 December 2000, OJ European Communities L 12/1.
203 Regulation (EC) 593/2008 of the European Parliament and of the Council of 17 June 2008 on the Law Applicable to Contractual Obligations (Rome 1) OJ European Communities L 177/6.
204 See recitals 19 & 22 of the E-commerce Directive.
205 Regulation (EU) No 1215/2012 of the European Parliament and of the Council of 12 December

member states. The Brussels Regulation was adopted to provide a legally binding instrument with direct application in furtherance of the Brussels Convention.[206] By this Regulation, jurisdiction in consumer contracts is easily discernable and judgments in any EU member state can be enforced throughout the EU, thus mitigating the problems consumers may face in enforcing judgments against suppliers in any EU member state.

The Brussels Regulation harmonises the jurisdictional rules of EU member states and applies to civil and commercial matters within the EU. Article 4 of the Brussels Regulation is a general jurisdiction clause in terms of which persons domiciled in a member state must, whatever their nationality, be sued in the courts of that member state. In cases where however, performance will take place in another jurisdiction, article 5 provides that a party can be sued in the country other than that in which he or she is domiciled.[207] However, jurisdiction in consumer contracts tend in favour of consumers on the ground that the consumer is a weaker party.[208]

Article 7(1)(a) of the Brussels Regulation contains a special jurisdiction clause which provides that a person can be sued in a court of a different member state, based on the place of performance of the contractual obligation. The place of performance of the obligation is defined in article 7(1)(b) as "the place in a member state under the contract where the goods were delivered, or should have been delivered, in a contract of sale, or if in a service contract, the place in a member state where, under the contract, the services were provided, or should have been provided." Article 7(5) also provides that where disputes arise out of the operations of a branch, agency, or other

---

2012 on Jurisdiction and the Recognition and Enforcement of Judgements in Civil and Commercial Matters (the Brussels Regulation) *OJL* 351,20.12.2012, P 1-32 this regulation is a recast of EC44/2001 published in *OJ* L12 of 16 January 2001 on Jurisdiction and the Recognition and Enforcement of Judgments in Civil and Commercial Matters.

206 The Brussels Convention was concluded on 27 September 1968 to address issues on jurisdiction and the enforcement of judgments in civil and commercial matters in the European Community.

207 See Brussels Regulation recital 11 and art 5. See also, Magnus & Mankowski *Brussels 1 Regu lation* (2007) art 2 para 5; art 23 paras 1-2.

208 Brussels Regulation recital 18.

establishment, a person domiciled in a member state may be sued in another member state in courts that have jurisdiction over the place where the branch, agency, or other establishment is located. In line with this provision suppliers can be effectively sued in the place of performance which is usually the location of the consumer.

However, jurisdiction over consumer contracts is specifically dealt with in Section 4, articles 17-23. Article 18 and 19 provides that a consumer may institute proceedings against the other party to a contract either in the courts of the consumer's home country, or in the courts of the member state where the supplier is domiciled. However, the supplier may only institute proceedings against a consumer in the courts of the member state in which the consumer is domiciled. The above notwithstanding, parties may deviate from these provisions by mutual agreement.[209] The purpose of article 18 of the Brussels Regulation is to ensure certainty and predictability of result by applying the mandatory rules of the consumer's habitual place of residence.

In terms of the Brussels Regulation consumer contracts do not include a transportation contract simpliciter.[210]

Articles 17-19 of the Brussels Regulation provide extensive protection for consumers. Clauses ousting the jurisdiction of the court are generally invalid unless the parties agree on a choice of jurisdiction after the dispute has arisen.[211] Same protection applies where they were both resident within the same jurisdiction and had at the beginning of negotiations entered into an agreement subject to the jurisdiction of that state in which they were both resident.[212] The provisions of the Brussels Regulation are specific, non-ambiguous, and apply directly to consumers within the meaning of the Regulation. It applies also to consumers' trade online within article 17(1)(c) which

209 Brussels Regulation art 19; Schulze (2006) 18 *SA Merc LJ* 38.
210 Brussels Regulation art 17(3).
211 Seaman 2000 *Computers and Law* 28-37; see also, Reed & Angel *Computer Law* 230.
212 Brussels Regulation art 19.

provides for contracts in "all other cases,"[213] in addition to contracts for the sale of goods on credit and contracts for a loan by consumers.[214]

The Brussels Regulation, however, creates exclusive jurisdiction in specific courts in respect of certain cases, including consumer contracts, regardless of the domicile of any of the parties. A list of the issues subject to exclusive jurisdiction, however, falls outside the scope of e-commerce-regulated activities and does not therefore constitute an obstacle to the protection of e-commerce consumers. The list includes proceedings involving immovable properties; validity of a Constitution or entries in public registers; patents and similar rights; dissolution of a company or legal entity; and the enforcement of a judgment.[215]

Finally, the general recognition and enforcement of judgments in the EU is regulated thus providing an effective chain of redress for e-commerce consumers in Europe.[216]

4.3.4 Implementation of e-commerce consumer protection principles in Europe and the Organisation for Economic Co-operation and Development

The Consumer Protection Guidelines [217] expressly recommends that consumer protection enforcement agencies should have appropriate authority[218] to investigate and protect consumers from fraudulent and deceptive commercial practices within their own territories [219] and also have capacity to protect foreign businesses. [220] However, the authority of the consumer protection enforcement agencies may be subject to other arrangements by member states.[221]

---

213 "All other cases" is interpreted in this study to include online contracts.

214 See art 17, Brussels Regulation.

215 Brussels Regulation art 24.

216 Brussels Regulation art 36.

217 Consumer Protection Guidelines para V.

218 Their authority should include administrative, civil and criminal enforcement powers as well as powers to grant restitution, the paper on *Consumer protection enforcement* highlights these powers and states that only a minority of the OECD states has civil or criminal enforcement powers see OECD *Consumer protection enforcement* 5.

219 Consumer Protection Guidelines para V(a).

220 Consumer Protection Guidelines para V(b).

221 Consumer Protection Guidelines para V(d); in addition, enforcement with non-EU members has

In line with the above guidelines of the OECD, the implementation plan under the E-commerce Directive directs that codes of conduct are required to be drawn at community level with the full involvement of all stakeholders. Member states are also required to have adequate means for supervising the activities of service providers, and to that end, to set up several contact and access points for dispute resolution and redress especially through online platforms. Currently, there is a Regulation on Consumer Protection Cooperation[222] known as the "CPC Regulation." The Regulation links the national competent authorities from all countries of the European Economic Area to form a "CPC Network" for ease of enforcement.[223] In each country there is a single Liaison Office to ensure the coordination of and cooperation between national authorities on different areas such as "unfair commercial practices, e-commerce, comparative advertising, package holidays, timeshare, distance selling, and passenger rights."[224] Authorities in the CPC Network do also have investigative and enforcement powers. Every year, the Network mobilises itself and carries out massive enforcement activities, called "sweeps." In a sweep, authorities simultaneously check, on the basis of a common check-list, whether a selected on-line sector complies with consumer rules and, if not, act on any breaches detected.

As regards disputes, bodies responsible for out-of-court settlement are required to be clear in their procedures, including instances where the operations involve appropriate electronic means.[225] The E-commerce Directive also enjoins member states to ensure that whatever court actions are used, infringements should be adequately addressed

been challenging due to the non-existence of international agreements with countries outside the EU, see OECD "Conclusion of the review of the 2003 Recommendation" 5.

222 CPC Regulation (EU) 2017/2394, this new Regulation became applicable on 17 January 2020 and replaced Regulation (EC) 2006/2004 on Consumer Protection Cooperation.

223 Preamble to CPC Regulation para 4.

224 EU "Consumer Protection Cooperation Network" available at https://ec.europa.eu (date of use: 28 July 2020).

225 E-commerce Directive art 17.

without delay.[226] The E-commerce Directive further provides for civil sanctions for infringement of any of its provisions as implemented in national laws.[227]

In addressing the enforcement of EU consumer protection laws it is essential to identify the role of negotiators or judges in interpreting and applying the principles of law. To date, bodies such as the Consumer Protection Network under the CPC Regulation and the European Commission Center for Complaints and Enquiries have been identified as implementing bodies. Decisions made by these bodies and other authorised bodies such as ADR agencies,[228] are enforceable anywhere in Europe.[229] Courts and alternative dispute resolution centers play enormous roles in implementing consumer protection measures. These roles are considered below.

(a) The role of the European Union Court within the European Union

The European Union Court established in 1952[230] interprets EU laws to ensure that they are applied uniformly across the EU countries. What this achieves for consumers is that enforcement of consumer protection principles is ensured and guaranteed. There is the Court of Justice and the General Court which is constituted by one judge from each EU country.[231] There is also the Civil Service Tribunal Court which is made up of seven judges.[232] The Court of Justice of the European Union (CJEU)[233] undertakes the functions of interpreting and validating EU law as contained in national legislation.[234] A national law can also be reviewed to determine whether it is compatible with an EU law. An EU Act that is believed to violate the EU

226 E-commerce Directive art 18.
227 E-commerce Directive recital 54.
228 ADR agencies are bodies entrusted with the onerous task of protecting consumers through user -friendly, multilingual, and accessible dispute-resolution platforms. These bodies, however, may at times need to rely on judicial processes to register their decisions before enforcement, on procedures for enforcement see Pablo *Online dispute resolution* 35.
229 This is achieved through mutual assistance see CPC Regulation arts 11-14.
230 Europa "Court of justice of the European Union (CJEU)" available at https:///www.europa.eu (date of use: 28 October 2020).
231 Europarl "The court of justice of the European Union" available at https://www.europarl.europe.eu (date of use: 28 October 2020).
232 Ibid.
233 Europa "Court of Justice of the European Union (CJEU)" available at http://europa.eu/about (date of use: 02 October 2020).
234 EU "The institution" available at https://curia.europa.eu (date of use: 03 October 2020).

treaty or fundamental rights can be annulled. Besides the Council or a member state, the request to annul an act can be made by an individual who is directly affected.[235] Other functions of the CJEU include reviewing the legality of actions of EU institutions and ensuring that member states fulfil their obligations under EU law.[236]

(b) Alternative dispute resolution

In administering justice, it has become a reality that court processes are cumbersome especially in trans-border transactions. In response, ADR and ODR have proven to be more effective methods of resolving disputes.[237] The rules are simpler and the agreement of parties, especially the consent of a natural party or consumer, is sacrosanct in the entire process. In 2013, the EU issued a Directive on Alternative Dispute Resolution for Consumer Disputes (Directive on Consumer ADR)[238] with the object of effectively sanctioning and enforcing ADR in consumer contracts. ODR rules became applicable in October 2015 and it was expected that ADR entities should be in full operation by 15 February 2016.[239] By this date, ADR bodies were to sign up for and familiarise themselves with the system. They were also expected to draw the attention of consumers to the existence of the platform.[240]

The Directive on Consumer ADR covers any entity "which offers the resolution of a dispute between a consumer and a trader through ADR procedures"[241] on an on-going basis. EU states are required to establish residual ADR entities in order to achieve an equitable geographic spread. An entity registered in one country should be able to

235 Vesterdorf "Proceedings of the Court" 118.

236 IJR "Court of Justice of the European Union" available at https://ijrcenter.org (date of use: 18 October 2020).

237 Pablo *Online dispute resolution* 3.

238 Directive 2013/11/EU of the European Parliament and of the Council of 21 May 2013 on Alternative Dispute Resolution for Consumer Disputes and amending Regulation (EC) 2006/2004 and Directive 2009/22/EC *OJL* 165,18.6.2013 63-79.

239 Pinsent Masons "Online dispute resolution platform now operational" 18 February 2016 available at www.pinsentmasons.com (date of use: 18 October 2020).

240 The ODR bodies became operational since 15 February 2016 and between then and February 2017, consumers had submitted over 24 000 complaints on its platform; see also Gelder and Biard "Functioning of the ODR Platform".

241 Preamble to Directive on Consumer ADR para 20.

operate directly or through a pan-European entity in another country.[242] States are further required to legislate on procedures regarding the settlement of disputes out-of-court, the duration of ADR procedures, the legal effect of their outcomes, and the enforceability of ADR decisions. The entities are, however, permitted to set their own procedural rules on fees, length of time before a dispute is presented, and similar procedural rules which must be reasonable so as not to deny consumers access to the service. All services offered by the entities must be fair, effective, and transparent.[243]

In terms of the Directive on Consumer ADR, services provided under the following circumstances are not acceptable ADR platforms.

(i) Out-of-court settlements "on an *ad hoc* basis for a single dispute between a consumer and a trader."[244]
(ii) Entities operated by the trader with employees who are exclusively remunerated by the trader.[245]
(iii) Settlement attempts made by a judge "in the course of judicial proceedings concerning the dispute."[246]

The Directives and Regulations in force in the EU are implemented by national laws of EU countries. It is therefore essential to consider the level of compliance of the E-commerce Directive and CRD in some EU countries as a means of measuring their application across board. For this purpose, laws implementing the EU Directive and the CRD in the UK will be discussed briefly. The objective of this is to evaluate whether the actual protection of EU nationals in their various countries reflects the standard which is provided for in the various EU Directives and Regulations on the protection of e-commerce consumers.

242 Directive on Consumer ADR art 26.
243 Directive on Consumer ADR art 5.
244 Preamble to the Directive on Consumer ADR para 20.
245 Ibid.
246 Ibid; see also Directive on Consumer ADR art 2.

4.4 The United Kingdom

A comparative study of the law, especially in a subject with international application, is an important tool in both research and the development of legal frameworks for international standards thus reference to the UK is relevant to this study. The UK is an ancient monarchy which has through its erstwhile "Empire-building," influenced the development of legal systems across the world, including in Africa, and, more specifically, Nigeria. The UK is made up of England, Wales, Scotland and Northern Ireland. Since October 2009, the Supreme Court has exercised jurisdiction over the entire UK.[247]

So far, the study of principles which must be established in every jurisdiction where the internet is accessed, has led to the conclusion that some consumer protection principles have gained international recognition through widespread application especially those contained in the UNCITRAL Mode Law and the EC Convention and that anything less would amount to inadequate legislative protection. Similarly, it has been shown that there are certain consumer-protection principles that have generally not been addressed in legislative instruments, and that these principles are key to ensuring a comprehensive consumer protection regime.

Before now, the UK was a member of the European Union (EU). By this status EU laws formed part of its regulatory framework as a direct source of law following the European Communities Act of 1972.[248] However, during this research, the UK embarked on the process of exiting the EU,[249] and the process was completed.

247 Supreme Court "Role of the Supreme Court" available at http://www.supremecourt.uk (date of use: 01 October 2020).

248 Elliot (2017) 76/2 *Cambridge Law Journal* 269.

249 The process of leaving the EU is the invocation of art 50 of the Lisbon Treaty which is an agreement spelling out how an EU member state may quit the EU by notifying the European Council and negotiates its withdrawal. This process may take two years unless everyone agrees to an extension. During this period, the exiting state will continue to apply EU treaties and laws but will however, not take part in any decision making, see BBC News "Article 50: UK set to formally trigger Brexit process" 29 March 2017 available at www.bbc.com 29 March 2017 (date of use: 16 October 2020).

Nonetheless, the UK's legislative experience in the EU can be relied on as a standard by which to assess the application of EU Regulations on e-commerce and consumer protection in the region. In the EU, e-commerce is controlled by the legislative framework of the EU internal market which member states are to implement nationally. In compliance, the UK adopted such Regulations and Directives. The UK's regulatory framework for consumer protection in the context of EU laws is, therefore, considered in this chapter.

4.4.1 Regulatory framework

The UK which was previously a part of the EU implements the various Directives and Regulations of the EU through her Regulations.[250] In the UK, consumer protection is regulated under the Electronic Commerce (EC Directive) Regulations,[251] which implement the E-commerce Directive, 2000; and the Consumer Contracts (Information, Cancellation and Additional Charges) Regulations,[252] which came into force in June 2014 implementing the Consumer Rights Directive (CRD). Section 19 of the CRD is further implemented by the Consumer Rights (Payment Surcharges) Regulations.[253] Consumers are specially protected by the Unfair Terms in Consumer Contracts Regulation,[254] which implements the Directive on Unfair Terms in Consumer Contracts.[255] Implementing the Unfair Commercial Practices Directive[256] is the Unfair Trading Regulations[257] while provision for cryptographic services is contained in the

250 Giliker (2015) 1 *European Review of Private Law* 5.

251 2002 No. 2013 Electronic Communications-The Electronic Commerce (EC Directive) Regulations 2002.

252 2013 No. 3134 Consumer Contracts (Information, Cancellation and Additional Charges) Regulations, 2013.

253 2012 No. 3110 Consumer Rights (Payment Surcharges) Regulations, 2012.

254 1999 No. 2083 Unfair Terms in Consumer Contracts Regulation, 1999.

255 Council Directive 93/13/EEC of 5 April 1993 on Unfair Terms in Consumer Contracts *OJL* 95, 21.4.1993, 29-34.

256 Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council (Unfair Commercial Practices Directive) *OJL* 149/22 11.6.2005.

257 2008 No 1277 The Consumer Protection from Unfair Trading Regulations 2008 amended by 2014 No. 870 The Consumer Protection (Amendment) Regulations 2014.

Electronic Communications Act;[258] this Act gives e-signatures the force of law.[259] Enforcement of consumer protection issues especially for online users is effected through the Brussels Regulation on Jurisdiction and Enforcement of Foreign Judgments. In addition to the Regulations mentioned above, consumers are generally protected under the Consumer Rights Act.[260] This Act is a broad piece of legislation offering protection to both online and offline users. Although not an area of discussion in the context of e-transactions per se, Chapter 3 of the Act deals concisely with the protection of e-commerce consumers through its provisions on digital content and interoperability. Interoperability is, however, further addressed by the Consumer Contracts (Information, Cancellation and Additional Charges) Regulations, 2013.

4.4.2 Electronic Commerce (EC Directive) Regulations 2002

Consumers in the UK are protected under the Electronic Commerce (EC Directive) Regulations, 2002, which implement the EU's E-Commerce Directive in UK law. The Regulations provide for Information Society Services. These services are defined as any service normally provided for remuneration at a distance, by means of electronic equipment for the processing (including digital compression) and storage of data, at the individual request of a recipient of the service.[261] This definition appears to have limited the application of the Regulations to commercial transactions. However, the UK's Department of Trade and Industry (DTI) – now known as the Department for Business, Innovation and Skill,[262] is of the view that the Regulations cover more than e-commerce businesses only.

According to the DTI guidance on the Regulations:

258 Electronic Communications Act 2000 Ch0700.
259 Wright "Electronic contracting" 3.
260 Consumer Rights Act, 2015.
261 E-commerce Regulation reg 2.
262 DTI *A Guide for Business to the Electronic Commerce (EC Directive) Regulations 2002* (2002) para 2.16 p 9 available at www.out-law.com (date of use: 16 October 2020).

> The requirement for an information society service to be "normally provided for remuneration" does not restrict its scope to services giving rise to buying and selling online. It also covers services (in so far as they represent an economic activity) that are not directly remunerated by those who receive them, such as those offering online information or commercial communications (e.g. adverts) or providing tools allowing for search, access and retrieval of data.[263]

4.4.2.1 Provisions

The E-commerce Regulations provide information requirements for service providers, rules on commercial communications, and e-contract rules. The Regulations apply to B2C and B2B e-transactions.[264]Further rules on confirmation and correction of errors amongst others are also contained in the Regulations and they adequately reflect the same standards as those in articles 5, 6 and 10 of the E-commerce Directive.[265]

Implementation of consumer protection measures are covered in articles 16 – 20 of the E-commerce Directive. This reflects in the Regulations which provide that consumers may obtain injunctions against service providers or sue them for damages, breach of statutory duties, or other applicable relief.[266]

4.4.2.2 Exclusions

The Regulations do not apply to taxation; information society services involving data protection; telecommunications; and privacy in e-communication.[267] They also find no application in regard to agreements on cartel law, activities of public notaries or similar professions, the representation and defence of clients in court, betting, gaming, or lotteries which involve wagering a stake with a monetary value.[268]

263 E-commerce Regulation reg 2.
264 E-commerce Regulation reg 9.
265 See E-commerce Regulation regs 6, 7, 8 and 15.
266 E-commerce Regulation reg 13.
267 E-commerce Regulation reg 3 compare with art 5 of the E-commerce Directive.
268 E-commerce Regulation reg 3 compare with art 9 of the E-commerce Directive.

4.4.3 Consumer Contracts (Information, Cancellation and Additional Charges) Regulations 2013

The Consumer Contracts Regulations (CCRs) apply to consumer contracts and implement the Consumer Rights Directive, 2011.[269]

4.4.3.1 Provisions

In the UK certain rights and principles have been earmarked for consumer protection under the CCRs. These principles are expected to reflect the principles contained in the CRD, specifically those relating to information, cancellation, and the prohibition of additional charges. These rights or principles are available to e-commerce consumers irrespective of the electronic medium used, which could be e-mail, webpage, mobile application, the internet, or any means of EDI. These special rights are necessary to bridge the gap created between e-consumption and conventional commerce.

In the CCRs, seven principles specific to the protection of e-commerce consumers are identified. They are principles governing information requirements;[270] use of e-contracts (confirmation and ordering procedure);[271] withdrawal and cancellation;[272] refund;[273] inertia selling;[274] additional charges;[275] and delivery.[276]

---

269 CCRs reg 3.

270 The principles provide that before a consumer enters into a contract online, he or she must be furnished with accurate information on a durable medium. The CCRs define a durable medium as a "paper or email or any other medium that allows information to be addressed personally to the recipient; that enables the recipient to store the information in a way accessible for future reference; or that allows the unchanged reproduction of the information stored," see reg 5. A list of this information is provided in Schedule 2 to the Regulations lettered (a)-(x) Information which suppliers must provide include (where applicable) information on the characteristics of the goods or services; identity of the trader; his/her geographic address, fax and telephone number, e-mail address; total price; delivery charges, arrangements for payment, delivery and performance; trader's complaint handling.

271 The Regulation recognises the use of electronic means for the conclusion of a contract and provides that confirmation must be on a durable medium. Non-provision of mandatory information by a supplier could nullify a contract see Reg 16 and 19.

272 The regulation reinforces the right of consumers to withdraw from a contract within a cooling-off period. These provisions as contained in regs 29-35 of the CCRs align with arts 9 and 14 of the CRD thus achieving uniformity for members of the EU.

273 Ancillary to the right of cancellation is the right to a refund and the refund should take place not

4.4.3.2 Exclusions

The Regulations do not apply to gambling contracts, which include gaming, betting, and participation in a lottery. They also do not apply to financial services; the creation of rights in immovable property; the construction of new buildings; or the supply of foodstuffs, beverages or goods for current consumption that are supplied regularly.[277] Package travel, holidays and tours, time share, long-term holiday products, and resale and exchange agreements are also not transactions which fall within the purview of the Regulations.[278] Furthermore, in terms of regulation 6, the CCRs do not apply to contracts concluded by means of automatic vending machine or automated commercial premises; with a telecommunications operator; or for the use of a single telephone, fax, or internet connection that is established by a consumer; and to contracts under which goods are sold by way of execution or otherwise by authority of law.

later than fourteen days from the date on which the goods are received, or not later than fourteen days after the date on which the consumer supplied evidence of having returned the goods, whichever is earlier see CCRs reg 34.

274 Consumers do not need to pay for unsolicited items or be responsible for their safe keeping see CCRs reg 39.

275 This is one of the additional safeguards in the Regulations which did not appear in the previous E-commerce Regulations, 2002. In here, suppliers are not permitted to levy additional charges beyond those presented as the cost of the goods, or charge consumers, in excess of regular rates for helplines or commercial lines, see CCRs Regs 40 & 41; Chirita "The impact of Directive 2011/83/EU" 21.

276 CCRs reg 42. Goods must be delivered not more than 30 days after conclusion of a contract or the contract will be terminated. Risk in goods remains with the supplier until delivery. The Reg however, fails to restate the requirement in the CRD which empowers consumers to allow the suppliers more time to perform the contract where they are not able to meet the 30-day delivery period.

277 CCRs reg 6, these exclusions are as contained in art 3(3) of the CRD.

278 CCRs reg 6(1)(g).

4.4.4 Unfair Terms in the Consumer Contracts Regulations 1999 and Consumer Protection from Unfair Trading Regulations 2008

Unfair terms are contracted terms that were prepared in advance without the input of the consumer, and which, "contrary to the requirement of good faith,…causes a significant imbalance in the parties' rights and obligations arising from the contract, to the detriment of the consumer."[279]

An unfair term or notice in a consumer contract is not binding on the consumer.[280] In the UK, unfair terms are regulated under the Unfair Terms in Consumer Contracts Regulations, 1999, (Unfair Terms Regulations) which revoke the Unfair Terms in Consumer Contracts Regulations, 1994. The Unfair Terms Regulations implement the EU Directive on Unfair Terms in Consumer Contracts.

4.4.4.1 Provisions

The Regulations apply to unfair terms in a contract between a seller and a consumer, and to a contractual term that is shown not to have been individually negotiated, notwithstanding that it forms part of an individually negotiated contractual term.[281] The burden to show that a contractual term was individually negotiated rests on the seller. In considering whether a contractual term is unfair, account must be taken of all the circumstances surrounding the conclusion of the contract without regard to the definition of the main subject matter of the contract, or the adequacy of the price or remuneration as against the goods or services supplied in exchange, provided that the relevant terms are recorded in plain, intelligible language.[282]

279 Unfair Terms Regulation reg 5; see also Booys & Hesselink "EU contract Law" 13.
280 Unfair Terms Regulation reg 8.
281 Unfair Terms Regulation regs 4 and 5.
282 Unfair Terms Regulation reg 6.

Contractual terms will be deemed unfair when they exclude or limit the legal liability of a supplier in the event of the death or personal injury of the consumer.[283] Such terms could also exclude liability where there is total or partial non-performance by the seller. Unfair terms enable a seller to alter the terms of a contract unilaterally without a specific or valid reason, or unilaterally to alter the characteristics of the product or service to be provided. In all circumstances unfair terms are terms that cause surprise or undue hardship to the consumer.[284] Whenever a term is found to be unfair, it has no binding effect on the consumer and can be disregarded, irrespective of whatever assent has been expressed by the consumer. Unfair terms will not be enforced by the courts, tribunals, or dispute resolution facilities.[285] A contract with an unfair term continues to bind the parties without the application of the unfair term if the contract can continue without that term.[286]

In a contract where there are terms which could be applied in non-member states, the Unfair Terms Regulations will apply, provided the contract has a close connection with a consumer within the territory of a member state.[287] The Regulations can be enforced by the courts, the Director-General of Fair Trading, and any of the qualifying statutory public bodies.[288] The Director-General may consider any complaint made to him or her about the fairness of any contract term drawn up for general use. He or she may, if it is considered appropriate to do so, seek an injunction to prevent the continued use of that term or of a term having like effect.[289]

Any of the qualifying bodies specified in Schedule 1 to the Regulations, may apply for an injunction to prevent the continued use of an unfair contract term provided it has informed the Director-General of its motion to do so at least fourteen days (or less with the permission of the Director-General) before the application is made. Upon a

283 Unfair Terms Regulation para 1 of schedule 2.
284 Unfair terms are specified in Schedule 2 to the Regulations.
285 Unfair Terms Regulations reg 8(1).
286 Unfair Terms Regulations reg 8(2).
287 Unfair Terms Regulation reg 9.
288 The statutory public qualifying bodies are made up of statutory regulators, trading standards departments, and consumer associations.
289 Unfair Terms Regulations regs 10 and 12.

complaint, the Director-General or a qualifying body under the Regulations may exercise their power to consider whether a contract term or similar term is unfair, and to establish whether a person has complied with an undertaking or a court order in respect of a contractual term concluded with a consumer.[290]

In considering a complaint about a term, the court may also consider similar terms and upon application, grant any injunction on such terms as it thinks fit. Injunctions which are granted do not necessarily have to be restricted to the particular term in question but to similar terms or terms with likely effect.[291]

Closely associated with the Unfair Terms Regulations is the Consumer Protection from Unfair Trading Regulations (CPRs). As earlier stated, the CPRs implements the Directive on Unfair Business-to-Consumer Commercial Practices which applies to "unfair B2C commercial practices before, during and after a commercial transaction".[292] The CPRs considers the nature of information given to consumers to the extent of how the information affects their transactional decision.[293] Therefore unfair commercial practices such as misrepresentations, omission of material information, and aggressive or coercive commercial acts are prohibited[294] and punishable.[295] Consumers must however, be mindful of the limitation of time on proceedings for offences in terms of the Regulation. Offenders must be prosecuted within three years of the commission of the offence or not later than one year of the prosecutor becoming aware of the commission of the offence.[296]

290 Unfair Terms Regulation reg 13.
291 Unfair Terms Regulation reg 12(4).
292 Directive on Unfair Business-to-Consumer Commercial Practices art 3; for further discussion on the Directive see Schurr (2007) 38 *VUWLR* 142.
293 The CPRs defines transactional decisions as decisions taken by consumers to undertake or refrain from acting in relation to a transaction, reg 2(1).
294 CPRs regs 3-7.
295 CPRs regs 8-13.
296 CPRs reg 14.

4.4.4.2 Exclusions

A breach of the Regulations will not invalidate an agreement or void contractual terms of a mandatory, statutory, or regulatory nature.[297]

4.4.5 Payment Services Regulations 2017

Secured payment systems are ensured in the UK following the implementation of the EU Payment Services Directive[298] by virtue of the Payment Services Regulations, 2017, (PSR) which entered into force between August and October 2017. The Regulations control the registration and administration of payment institutions and cover all electronic and non-cash payments ranging from credit transfers, direct debits, and card payments. Part 6 regulates information requirements for payment services as performed by payment service providers (PSP).[299]

4.4.5.1 Provisions

The Regulations require that consumers are given specific, accessible, and easily comprehensible information by the PSP before and after the services are used.[300] Before a payment transaction is concluded, the PSP must make available to the user, information on the payee, amount in the transaction, currency and exchange rate where applicable, and the date on which the payment order was received.[301] After executing the payment order the PSP must inform the user of the amount involved in the transaction, and the credit value date and charges related to the transaction.[302] Consumers have a right to refund where there is unauthorised debit of the consumer's

297 CPRs reg 29.
298 Directive 2007/64/EC of the European Parliament and of the Council of 13 November 2007 on Payment Services in the Internal Market. The Directive applies in 30 European countries of the EU, Iceland, Norway, and Liechtenstein.
299 Payment service providers include payment institutions like the money remitters, retailers, banks, and phone companies, see PSR reg 2.
300 PSR regs 43, 44 and 46.
301 PSR reg 45.
302 PSR reg 46.

account, overcharging and incorrect processing.[303] The PSR is regulated by the Financial Conduct Authority.[304]

4.4.6 Limitations in UK Regulations

A closer look at the E-commerce Regulation shows that, unlike the Directive on E-commerce, the E-commerce Regulation does not provide for opt-out registers for natural persons in respect of unsolicited commercial communications. This is, however, taken care of by the "Do-not-call list" in the UK where the Telephone Preference Service (TPS) is used by subscribers to block unwanted calls.[305]

The Consumer Contracts Regulation also omitted to provide consumers with the leverage to allow additional time within which suppliers may deliver goods or perform the contract in cases where they are unable to meet the required 30-day period. As minor as these omissions may appear, it is cardinal that the level of protection provided in consumer contracts is uniform throughout the EU.

In light of the oversights highlighted above, a trite issue of law arises as to whether the UK regulation, or the provisions of the EU Community laws, will be enforced where there is interaction or conflict between them in respect of a consumer in the UK. In resolving this issue, recourse is had to the pronouncements of the European Court of Justice in a matter brought before it by the House of Lords. In the case of *The Queen v Secretary of State for Transport, ex parte: Factortame Ltd and others*,[306] the House of Lords, in deciding whether the national court was correct in its decision to grant interim relief where the issue before it involved Community law; took the view that the dispute before it involved interpreting Community law, and decided, pursuant to article 177 of

303 PSR regs 74, 76 & 79.
304 PSR reg 4.
305 Telephone Preference Service "Welcome" available at https://www.tpsonline.org.uk (date of use: 20 October 2020).
306 *The Queen v Secretary of State for Transport, ex parte: Factortame Ltd and others*, Case C-213/89 ECR 1990 1-02433 (hereafter the *Queen* case).

the EEC Treaty, to hold on for a preliminary ruling on the issues raised. In its reply, the ECJ[307] referred to the case of *Administrazione delle finanze dello Stato v Simmenthal SpA*[308] where the court held that,

> directly applicable rules of community law, 'must be fully and uniformly applied in all the member states from the date of their entry into force and for so long as they continue in force' and that 'in accordance with the principle of the precedence of Community law, the relationship between provisions of the Treaty and directly applicable measures of the institutions on the one hand and the national law of the member states on the other hand is such that those provisions and measures by their entry into force render automatically inapplicable any conflicting provision of national law.[309]

The court consequently held as an obstacle to Community law, any provision of a national law that could prevent Community law from having its full force and effect and should be set aside.[310] Thus it is settled that omissions in the UK Regulations notwithstanding, the rights of consumers are not adversely affected as they can always access their rights from Community laws which have direct application. States are actually under an obligation to transpose Directives to which they are party, or they could be liable for damages to affected persons due to poor or non-implementation.[311]

4.4.7 Enforcement and implementation in the United Kingdom

In the UK it is the duty of every weights and measures authority in Great Britain, to enforce the CCRs within its area. It is also the duty of the Department of Enterprise, Trade and Investment in Northern Ireland to enforce the Regulations within Northern Ireland.[312]

Where an enforcement authority has reasonable grounds to suspect that an offence may have been committed under the CCRs, it may require that any document relating to the business be provided and may seize and detain such documents if required as

307 The *Queen* case para 18.
308 *Administrazione delle finanze dello Stato v Simmenthal SpA* (1978) ECR 629.
309 The *Queen* case para 18.
310 The *Queen* case para 23.
311 This principle was established in the case of *Francovich v Italy* Case C- 6/90 ECLI: EU:C:1991:428.
312 CCRs reg 23(1).

evidence. A person commits an offence where he or she intentionally obstructs or fails, without reasonable cause, to comply with any requirement under the Regulations, or fails to assist another who is carrying out enforcement activities under the Regulations. In order to secure compliance, an enforcement authority may apply for an injunction or interdict against any person and inform the Competition and Market Authority (CMA) of any such court order.[313]

In addition to the above, consumers in the UK can complain to an ombudsman service whenever issues arise. They can also approach the UK Department for Business, Innovation and Skills with all consumer-related complaints. Furthermore, when a UK consumer wishes to purchase goods or pay for services from a supplier from another EU member state, the consumer can contact the UK European Consumer Centre (ECC) for advice and information about the company abroad. The Centre handles complaints and intervenes in disputes if a consumer and a trader are unable to reach a positive outcome themselves. The UK ECC is co-funded by the UK and the EU.[314]

4.5 Australia

4.5.1 Background

Australia is a continent administered as a single country. Before considering the protection of e-commerce consumers in Australia, it is important to note that, as with other jurisdictions, thought on consumer protection was initially not globalised. While consumers may enjoy protection in tort or contract under conventional sales-agreement provisions, consumer protection finds expression in the complexities attendant upon e-transactions. In Australia, specific legislation on consumer protection in relation to the electronic market dates back to the Electronic Transactions Act, 1999 (ETA). In addition to the ETA e-commerce consumers in Australia also enjoy protection

313 CCRs reg 46.

314 UKECC "What is the UK European Commission Centre" available at http://www.ukecc.net (date of use: 07 October 2020).

from the provisions of the Australian Consumer Law[315] which is administered by the Australian Competition and Consumer Commission (ACCC). The special feature of the ETA is that it applies in the nation, state, and territories of Australia. This is a special achievement in view of the Australian legal system.

Australia is a federation consisting of six states, three federal territories, and seven external territories. All states and two of the three internal territories have their own parliaments and administer themselves. All remaining territories are administered by the federal government (with Norfolk Island having some degree of self-government). Each of the States and Territories has its own parliament, Supreme Courts, and the police. Australia practices both democratic and monarchic systems of government having originated as separate British colonies prior to federation in 1901. Each state has a Governor, appointed by the Queen on the advice of the Prime Minister, while the Administrators of the Northern Territory and Norfolk Island are appointed by the Governor-General. The head of government of each state is called the Premier and is appointed by the State Governor.[316] The Commonwealth of Australia is the Federal Government, domestically administered by the Governor-General with the Prime Minister as head of government. It has direct ties to Queen Elizabeth II of the United Kingdom as its head of state.

Against this background of how the states and territories in Australia interact with one another and the Commonwealth of Australia, it is possible to comprehend the interdependence of the legislative process and law enforcement in Australia as a continent, and how this could affect, in particular, the legal framework regulating consumer protection in Australian states.

Without doubt, building a synergy of applicable laws within the states and territories is a formidable task that requires great skill if it is to further the uniformity of e-commerce

315 The Australian Consumer Law is contained in Schedule 2 to the Competition and Consumer Act, 2010 (CCA).

281 Australian Government "How government works" available at www.australia.gov.au/about-government (date of use: 13 October 2020).

rules. Fortunately, the law governing e-transactions was adopted as a uniform law in Australia so mitigating challenges that could have surfaced in differing applications of e-transaction rules within the continent.

4.5.2 Regulatory framework

E-commerce consumers are protected in Australia by a combination of private-sector codes from the Communications Alliance [317] and the Australian Direct Marketing Association (ADMA);[318] by Guidelines such as the Australian Guidelines for Electronic Commerce; [319] and above all by legislation; which is primarily the Electronic Transactions Act (ETA).[320]

4.5.3 Electronic Transactions Act 1999

The ETA is based on the UNCITRAL Model Law on Electronic Commerce, 1996,[321] which was adopted by most states and territories in Australia between 2010 and 2013. [322] Proposals for the amendment of the Electronic Transaction Act were introduced in the Australian House of Representatives on 9 February 2011, in order to update the Australian e-transaction legislation to reflect internationally recognised

317 Communications Alliance took over the industry codes and functions of the Internet Industry Association in 2014, available at www.commsalliance.com.au (date of use: 14 October 2020).

318 The Australian Direct Marketing Association (ADMA) is an Association for Data-Driven Marketing and Advertising see ADMA "About ADMA" available at www.adma.com.au (date of use: 14 October 2020).

319 Australian Guidelines for Electronic Commerce 2006.

320 Act 162 0f 1999, the Act was amended by the Electronic Transactions Amendment Act, 2011.

321 Tasneem (2011) *International Journal of Management and Business Research* 85; Christensen & Low (2004) 1 *Digital Evidence and Electronic Law Review* 40.

322 The UNCITRAL Model Law was adopted in Australia in 2011; Australian Capital Territory in 2012; New South Wales in 2010; Northern Territory in 2011; Queensland in 2013; South Australia in 2011; Tasmania in 2010; Victoria in 2011; and Western Australia in 2011, see "UNCITRAL Model Law on Electronic Commerce (1996) – status" available at www.uncitral.org (date of use: 28 October 2020).

standards in e-commerce as set out in the EC Convention.[323] Although Australia is yet to accede to the EC Convention, efforts are under way to finalise its accession.[324]

4.5.3.1 Provisions

The ETA applies to e-consumer contracts. It covers transactions of a commercial nature and any other e-transaction.[325] The Act, therefore, provides for commercial and non-commercial transactions and applies throughout the Commonwealth of Australia and in all its external territories.

An issue of primary concern in the ETA is that a consumer is not defined. It would be reasonable to refer to the provisions of the Australian Consumer Law 2010 (ACL) which is contained in Schedule 2 to the Competition and Consumer Act 2010 (CCA), but a look at the definition of "consumer" in section 3 of the ACL, raises a question. Under the ACL, a consumer is defined as a person who: acquires goods or services of an amount not exceeding 40 000 Australian dollars; or who acquires goods or services for personal, domestic, or household use or consumption; or who acquires a vehicle or trailer for use principally in the transport of goods on public roads. The acquisition must not be for re-supply, trade or commerce, or for the purpose of production, or manufacture.

The question arising is whether the definition of a consumer as contained in the ACL, would also apply to e-contracts. In the absence of any other definition within the regulatory framework of consumer protection in Australia, the definition as proposed in the ACL may apply. One point, however, is that by this definition, a consumer is defined in line with the usual expectations of a natural person.

---

323 Parliament of Australia "Electronic Transactions Amendment Bill 2011" available at https://www.aph.gov.au (date of use: 16 October 2020).

324 Australian Government "United Nations Convention on the Use of Electronic Communications in International Contracts" available at http://www.ag.gov.au (date of use: 04 October 2020).

325 See s 5(1) of the Electronics Transactions Amendment Act, 2011 (Australian ET Amendment Act).

The principles running through the ETA relate to the recognition of e-messages,[326] the validity of e-contracts, principles governing time and place of dispatch, and time and place of receipt. There are also principles on attribution of e-messages, the recognition of AMS and the correction of errors. These principles are discussed below.

(a) Recognition of electronic communications

Transactions are valid when they meet certain requirements under section 9 of the ETA.[327] Where the law requires that a document is written that requirement is met by means of an e-communication provided that at the time the information was given:

(i) It was reasonable to expect that the information would be readily accessible so as to be available for subsequent use.

(ii) It was given in accordance with the format specified by the recipient, that is, in accordance with particular information technology requirements,[328] or by means of a particular kind of e-communication or on a particular kind of storage device.

(iii) It was given in a way that it can be verified by receipt.

Writing, in terms of section 9(5) of the ETA, includes: “making an application; making or lodging a claim; giving, sending or serving a notification; lodging a return; making a result; making a declaration; lodging or issuing a certificate; making, varying, or cancelling an election; lodging an objection; or giving a statement of reasons”. An e-signature is recognised if it identifies the originator by a method that is reliable and appropriate for the purpose. An e-signature will also be recognised where it is used in accordance with a particular information technology described by the person or entity requiring it. Where documents need to be retained, they may also be retained electronically. These requirements apply to the production of documents except in respect of migration and citizenship documents, or documents relating to infringement of copyright.

326 See McNamara and O’Shea “Minimising legal risks in electronic contracting” 5.
327 Barber and Edghill (2006) 24/4 *Communications Law Bulletin* 24.
328 ETA s 9 (b).

(b) Principles governing contract formation

The ETA applies to the formation of and performance under a contract between parties, irrespective of the location of the parties or whether the contract is for business, personal, family, household, or other purposes. It applies where the applicable law is the law of an Australian state or territory in which, when the contract was concluded, there was no law of that state or territory, which corresponded substantially to the ETA.[329]

This provision reflects that the Commonwealth does not intend to legislate to "cover the field" in view of section 109 of the Australian Constitution which invalidates any state law that is inconsistent with a Commonwealth law. Rather, the Commonwealth intends to preserve the validity of an equivalent provision in any state or territory's legislation. The ETA, therefore, functions as a default rule in transactions governed by the law of a state or territory where no state or territory laws exist, or where the provisions in those laws are not substantially the same as the provisions of the Act. This aims to create uniformity for the whole of Australia.

The ETA contains the following principles on the formalities required of an e-contract.

(i) Time of receipt

Unless otherwise agreed by the parties, the time of receipt of an e-communication is the time the e-communication becomes capable of the being retrieved by the addressee at an electronic designated address, or if not at a designated address, it is deemed to have been received when it becomes capable of being retrieved by the addressee at another address and the addressee becomes aware that the e-communication has been sent to that address.[330] There is a presumption that an e-communication is capable of being retrieved by the addressee when it reaches the addressee's electronic address.

(ii) Place of dispatch and place of receipt

329 ETA s 15A.

330 ETA s 14A; see further Barber and Edghill (2006) 24/4 *Communications Law Bulletin* 25.

An e-communication is said to have been dispatched at the place where the originator has its place of business, and it is taken to have been received at the place where the addressee has its place of business. The determination of a party's place of business articulates the position in the UNCITRAL Model Law on E-commerce.[331] Section 14B of the ETA, as with other substantial parts; reflect the underpinnings of the UNCITRAL Model Law thus implementing its provisions. The section provides that a party's place of business is based on the address indicated, and where no address has been indicated, it is that place with the closest relation to the transaction. The ETA provides further, that where there is no place with a close relation to the business, and the party has more than one place of business, it is to be assumed that the party's principal place of business is its only place of business. If a party is a natural person who does not have a place of business, it is to be assumed that the party's place of business is his or her habitual place of residence.

The ETA further aligns with article 6 of the EC Convention in its definition of the location of parties. The ETA provides under section 14B (3), that a location is not a place of business merely because it is,

(a) where the equipment and technology supporting an information system used by a party are located; or
(b) where the information system may be accessed by other parties.

Furthermore, the sole fact that a party makes use of a domain name or e-mail address connected to a specific country does not create a presumption that its place of business is located in that country.

Although the Act gives an exclusive indication of the location of a party, the provision conforms to the general principle of the location of a party in e-commerce. The principle from our study so far, establishes that the location of a party is likened to the

331 Compare art 15(4) UNCITRAL Model Law with s 14B of the ETA; see also art 6 of the EC Convention.

place of establishment which is where a party directs his or her activities. In line with the ETA, mere access does not establish location; there must also be directed and purposeful activities in a place before it is regarded as a location.

(iii) Invitation to treat

The ETA provides that where a proposal to conclude a contract is addressed to more than one party and is generally accessible to parties making use of information systems, the proposal is to be regarded as an invitation to treat.[332] For instance, interactive applications in online-stores for the placement of orders, are mere invitations.

(c) Attribution of e-communications and general principles

The ETA provides in section 15 for the attribution of e-communications in line with article 13 of the UNCITRAL Model Law. Other similar provisions involve the use of AMS for contract formation, and the legal position in respect of errors in e-communications between a natural person and the AMS of another party. There are also provisions dealing with retention of e-communications and their reproduction. These provisions are on all fours with the principles reflected in the EC Convention.[333]

4.5.3.2 Exclusions

The ETA does not apply to specified acts in the Electronic Transactions Regulations.[334] These are regulations which apply to: banking and insurance contracts; taxes; aboriginal land rights; bills of exchange; chemical weapons; child support; elderly care; and corporations' law.[335] The use of data in the production of documents is generally allowed except in respect of migration and citizenship documents.[336]

---

332 ETA s 15b and compare with art 11 of EC Convention.
333 See art 14 EC Convention and art 10 of UNCITRAL Model Law.
334 Electronic Transactions Regulation 2000; see Christensen & Low (2004) 1 *Digital Evidence & Electronic Law Review* 40.
335 See Schedule 1 to the Electronic Transactions Regulation, 2000.
336 ETA s 11(2).

4.5.4 The Australian Guidelines for electronic commerce 2006

Besides the ETA, e-commerce consumers have a wide range of protective measures contained in the Australian Guidelines for Electronic Commerce. Although the principles in the Guidelines are not enforceable, they however, provide guidance.[337]

4.5.4.1 Provisions

The Guidelines apply to B2C transactions to the exclusion of private communications between individuals in a non-business relationship. The Guidelines provide rules on "fair business practices; accessibility and disability access; advertising and marketing; engaging with minors; disclosure of business's identity and location;"[338] contract terms; and the adoption of privacy principles amongst other principles.[339]

4.5.5 Limitations of e-consumer protection instruments in Australia

While consumer protection under the ACL does not fall within the scope of this work, e-commerce consumers will have to rely on substantive rules provided in the ACL in areas where there are gaps in the ETA. The ACL provides adequate protection for consumers against unsolicited goods also referred to as inertia selling. It provides that unsolicited goods or services are not subject to payment or liability for loss or damage unless the person in possession of the goods or services unreasonably refuses to permit the owner or sender of the goods or services, to take possession during the recovery period of three months starting from the day after the goods are received. If the receiver of the unsolicited goods gives the supplier written notice, the recovery period ends one month after the day on which the notice is given. The ACL also prohibits a person from sending an invoice or other document stating the amount due for payment for the supply of unsolicited goods or services.[340] Demanding payment for

337 The Australian Guidelines for Electronic Commerce 2006 v.
338 The Australian Guidelines for Electronic Commerce para 10.1 - 10.5.
339 The Australian Guidelines for Electronic Commerce para 10.
340 ACL s 40.

unsolicited goods or services attracts a penalty of 1 100 000 Australian dollars for a body cooperate, or 220 000 Australian dollars for an individual.[341]

As regards unsolicited commercial communications, provision is made for a do-not-call register, under the Do-not-Call Register Act, 2006. The ACL voids unfair contract terms under its section 23. In terms of secured payment, the ACL prohibits payment or deduction for supplies that were not delivered. It provides a penalty for a breach of that provision.[342]

On the whole, it has been shown that the framework for legal protection of e-commerce consumers in Australia is not comprehensive and would therefore benefit from reform.[343] The ETA substantially implements international standards in e-transactions as set out in the UNCITRAL Model Law and the EC Convention. Consumers in Australia will, however, benefit more from the incorporation of additional basic consumer protection principles contained in documents such as the E-commerce Directive and the CRD. These Directives recognise the rights of consumers to online disclosures,[344] withdrawal,[345] performance,[346] refund,[347] and protection from unnecessary charges,[348] amongst others. Under the Directives, consumers enjoy additional protection when using single-window facilities,[349] such as mobile phones, and there is also the obligation on suppliers to ensure the "interoperability of digital content with hardware and software".[350]

Based on the evaluation of the ETA in this chapter, it is clear that most aspects of e-commerce consumer protection are not covered; and that certain provisions of the ETA

341 ACL s 162.
342 ACL ss 36 and 158.
343 Ha "Three-sector governance system" 11 available at www.anzam.org (date of use 14 October 2020).
344 E-commerce Directive art 5; see also Consumer Rights Directive (CRD) art 6.
345 CRD art 9.
346 CRD art 18.
347 CRD art 13.
348 CRD art 19.
349 CRD art 8(1)(4).
350 CRD art 6(1)(s).

are ambiguous. The intermittent application of certain parts of the ETA to state or territory laws makes its provisions clumsy. There is no clear division of the ETA into Parts 1 and 2. The ETA replicates the provisions of the UNCITRAL Model Law but does not build on them with the result that the defects in the UNCITRAL Model Law are repeated in the ETA. As observed by Tasneem[351] means of identifying and enforcing the legal capacity of contracting parties is not provided in the ETA. From the provisions of the ETA the challenge posed by spam or unsolicited communications, is not addressed. Spam has been a major concern in e-communications and was approximated as constituting half the size of e-mails in the world in 2005[352] and a loss of about 8.5 billion Australian dollars in monetary value of time and bandwidth in Australia.[353] To address this situation in 2003 the Spam Act with an amendment (Consequential Amendment Act) was passed into law.[354] The Spam Act addresses various concerns in spam and provides measures to curb them.

Although the ETA has limited coverage on consumer protection measures there is, however, a lot of benefits for consumers in the Australian Guidelines for Electronic Commerce. As earlier stated, the principles in the Guidelines are of limited value since they have no force of law.

4.5.6 Jurisdiction in Australia

As has been observed above, state or territory law of Australia applies to jurisdiction in e-contract cases where the contracts would otherwise have been governed by those laws. And where the state or territory laws are silent, Commonwealth law applies.[355] There appear to be no decided cases on internet jurisdiction in the area of e-commerce in Australia, but there is a case dealing with defamation where internet jurisdiction was in issue. In *Dow Jones & Company Inc v Gutnick,*[356] Dow Jones

351 Tasneem (2011) *International Journal of Management and Business Research* 86.
352 Quo (2004) 11/1 *Murdoch University Electronic Journal of Law* para 2.
353 Bender *Australia's spam legislation* 4.
354 Commonwealth Spam Act (Spam Act) 2003.
355 ETA ss 15E & F.
356 *Dow Jones & Company Inc v Gutnick* (2002) HCA 56 (210 CLR 575), 77 ALJR 255; 194 ALR

published an article online, part of which defamed Gutnick. Dow Jones had his server in New Jersey US, while Gutnick was domiciled in Victoria, Australia. Though he had businesses and engaged in charity work outside Australia, including in the US.[357] Gutnick brought his action in the Supreme Court in Victoria but Dow Jones contended that Victoria had no jurisdiction as the article had been published in New Jersey. His contention was based on the principle of single jurisdiction. The Supreme Court of Victoria found and assumed jurisdiction. Dissatisfied, Dow Jones attempted to appeal to the Court of Appeal of Victoria, but he was refused leave to appeal.[358]

By special leave, Dow Jones appealed to the High Court of Australia which commented that, although considerable emphasis is placed on the advent of the WWW representing a notable technological advance, the problem of widely-disseminated communications is far older than the internet and the WWW. The court stated that given the argument of the appellant (Dow Jones), the single publication rule in the US had been adopted to forestall multiple litigation in respect of a single case, and that where and when the case came up, the plaintiff could claim damages in respect of that publication wherever it was published without suing the defendant everywhere it had been published.[359] The court referred to the case of *Firth v State of New York*[360] in which the New York Court of Appeal referred to the first posting of defamatory matter on an internet site, and found that it went to the issue of the one-year statute of limitation which the court held should start running from the first posting of the defamatory matter.[361] The High Court of Australia held that in Australia, the choice of law to be made is principally the law of the place of the tort. Australian common-law choice of law rules do not require locating the place of publication of defamatory material, but only the place of the publisher's conduct. Defamation should

433 available at http://eresources.hccourt.gov.au (date of use: 13 October 2020) (hereafter *Dow Jones* case).

357 *Dow Jones* case para 2.

358 *Dow Jones* case para 3.

359 *Dow Jones* case see paras 38 & 57-58 of judgment; see also s 577A of the Restatement of Torts 2d (1977) "Single and Multiple Publications."

360 *Firth v State of New York* 775 NE 2d 463 (NY 2002) briefed in Google scholar available at https:/scholar.google.com (date of use: 13 October 2020) (hereafter the *Firth* case).

361 *Dow Jones* case para 30; see also the *Firth* case 372.

be located at the place where the damage to reputation occurs because that is where the defamatory material is available in a comprehensive form. In this case, that was found to be where the material had been downloaded.[362]

Gutnick alleged to have suffered damages in Victoria as a result of the publication in Victoria and that the article was available to a reader in Victoria. On this basis, the High Court of Australia reaffirmed jurisdiction and dismissed the respondent's appeal.[363] This case affirms the principle that the court may assume jurisdiction in cases of defamation on the internet. Outside the location of the server, the courts have adopted the effects test to assume jurisdiction, this principle can also be applied in e-commerce cases.[364] It should be noted that the effects test is one of the principles applied in determining jurisdiction in the US courts, as seen in Chapter 6.

However, no jurisdictional issues will arise in Australia under the ETA, as State or Commonwealth jurisdictional rules apply throughout the Continent in respect of e-transactions – save where the transaction involves parties from jurisdictions outside Australia. Ordinarily, recourse should be had to international rules governing internet jurisdiction in e-commerce cases.[365] Unfortunately, however, there are currently no such rules.

4.5.7 Enforcement and implementation in Australia

In Australia all consumer complaints are treated by the Australian Competition and Consumer Commission (ACCC), a Commission created under the Competition and Consumer Act (CCA). Under the CCA implementation is central, thus making enforcement easier, predictable, and more efficient.

362 *Dow Jones* case para 9.
363 *Dow Jones* case paras 202-203.
364 See para 6.7.1(d) of Chapter 6 (above) on the effects test.
365 Ha "Three-sector governance system" 11 available at www.anzam.org (date of use 14 October 2020).

Where there are issues in payments especially with the use of cards, complaints can be made at the Credit and Investment Ombudsman for resolution.[366] Spam related complaints are handled by the Australian Direct Marketing Association (ADMA) which was established by the Australian Competition and Consumer Commission. The ADMA regulates its members who are basically suppliers and service providers through the provision of rules for the fair use of e-communications, opt-in models, and privacy.[367] There is also the Communications Alliance in Australia with a similar mandate to prohibit ISPs and other subscribers from direct communication in the absence of the recipient's consent.[368] Members of these associations who do not keep to the code are at the risk of having their membership revoked.[369]

Finally, the Australian system is outstanding in terms of implementation since the ETA is applied in all the states and enforcement is centrally deployed. This uniformity diffuses uncertainty and encourages consumer transactions online from whatever location within Australia.

4.6 Summary and conclusion

In this chapter, there has been a broad study of consumer protection in Europe. From it, the drivers for effective protection for e-commerce consumers have been identified as legislation and harmonisation. Harmonisation leads to trust, confidence, economic growth, and legal protection.[370] The existing regulatory structure in the EU drives a unification of laws across member states and presents an opportunity for the growth of e-commerce within the EU. It is certain that clarity on legal rules helps to build trust in consumers thus promoting e-commerce[371] and facilitating consumer protection. The 2003 report of the Commission on the application of the E-commerce Directive drives

366 CIO "Credit and Investment Ombudsman" available at http://www.cio.org.au (date of use: 13 October 2020).
367 Quo (2004) 11/1 *Murdoch University Electronic Journal of Law* para 17.
368 Quo (2004) 11/1 *Murdoch University Electronic Journal of Law* para 20.
369 Quo (2004) 11/1 *Murdoch University Electronic Journal of Law* para 18.
370 European Parliament *Towards new rules* 33.
371 European Commission "A Comprehensive Approach to Stimulating Cross-border e-Commerce for Europe's Citizens and Businesses" 2016 at 5.

home the impact of harmonisation on consumers. From the report there was a growth in internet usage by consumers from eighteen per cent to 43 per cent within two years. From another report, a 2007 report on the economic impact of the E-commerce Directive, it was observed that with the removal of the domestic-barrier index within the EU, most of the challenges to the use of e-contracts and issues surrounding the liability of service providers have been resolved. Service providers who were authorised to practice also had no barriers in being established in any EU jurisdiction.[372]

The E-commerce Directive was based on the "minimum harmonisation approach" which left room for differing standards at the national levels. The CRD, however, has to a large extent resolved issues which could arise from the minimum approach, by replacing it with mandatory standards.[373] Excessive charges by suppliers through payment schemes and communication channels have been eliminated by the CRD so providing greater protection for the consumer. There is also a standard timeframe for the application of the rights of withdrawal, delivery, and refund under the CRD.

At the beginning of this chapter, it was pointed out that the UK was under an obligation to implement EU laws on consumer protection in respect of e-transactions in its national law. The first step in qualifying this obligation is to ascertain whether there is UK legislation implementing the various EU e-commerce consumer protection laws. If there is, the next step is to identify whether the UK legislation adequately implements the EU provisions. The study has shown that every aspect of the EU regulatory framework on e-commerce consumer protection has received fair attention in UK legislation thus providing adequate protection for consumers in terms of EU law. It is submitted that the UK provisions on consumer protection are substantially in compliance with EU law thereby ensuring uniformity and predictability of consumer protection rules for UK consumers within the EU. The same cannot be said of the

372 Nielsen CK et al *Study of the Economic Impact of the Electronic Commerce Directive* 2007 10 (DG Internal Market and Service, European Commission). However, it was observed in the report that some websites did not comply with some information requirements.

373 See recitals 3 and 25 CRD.

Australian legal framework for the protection of e-commerce consumers. The ETA is substantially modelled after the UNCITRAL Model Law and not on EU Directives (that are relevant to consumer protection and e-commerce). The ETA falls short of most of the issues which have been addressed at the level of the EU and would therefore benefit from updating its legislation to enhance trade relationships with other regions.

In conclusion, the study of the different relevant Directives and Regulations for the protection of e-commerce consumers in the EU shows legal certainty. The level of certainty is particularly high in the area of cross border implementation and redress within the EU.

The following chapter, Chapter 5, focuses on Africa and the role of the African Union (AU), and some African regional bodies in providing consumer protection for e-commerce consumers in the continent of Africa. A practical application of e-transaction laws in African countries is also studied through the South African Electronic Communications and Transactions Act 2002 (ECTA) in South Africa.

CHAPTER FIVE

REGIONAL PROTECTION OF ELECTRONIC COMMERCE CONSUMERS: AFRICA

5.1 Introduction

The previous chapter examined the international framework for consumer protection and the regional protection of consumers in the EU and Australia. This chapter examines the existence of consumer protection in the electronic environment in Africa through the African Union Convention on Cyber Security and Personal Data Protection (AU Convention)[1] and other regional instruments on consumer protection. Thereafter, a practical evaluation of the possible influence of these instruments on African countries is undertaken by using South Africa as a case in point.[2]

While global e-commerce is edging towards newer technologies, it is shocking that certain countries in Africa are yet fully to experience the impact of the electronic age, due largely to poor infrastructure.[3] Developing countries also lag behind in the development of cyberlaw as "cross-border e-commerce is hampered by variations in the laws and regulations enacted in different countries."[4] In Africa as a continent, 32 countries have specific e-transaction laws, ten countries have draft legislation, and four countries have no legislation while there is no information on eight countries.[5]

---

1 African Union Convention on Cyber Security and Personal Data Protection 2014 adopted on 27 June 2014 available at https://au.int/en/treaties (date of use: 08 October 2020).

2 South Africa records a large number of internet penetration (about 55.5 per cent) following Nigeria with penetration rate of 61.2 per cent see Internetworldstats "World internet usage and population statistics 2020-Q1-March-updated" at www.internetworldstats.com (date of use 20 July 2020). However, unlike Nigeria, South Africa has since 2002 put in place an e-transaction specific legislation which embodies basic consumer protection principles as will be seen in para 5.8 of this chapter.

3 Ndonga (2012) 5 *African Journal of Legal Studies* 245; International Trade Center "International e-commerce in Africa" 10; Okoli and Mbarika "A framework for accessing e-commerce" 2, 14; Ewelukwa (2011) 13 *European Journal of Law Reform* 570.

4 UNCTAD, Expert Meeting on Cyberlaws and Regulations for Enhancing E-commerce, including Case Studies and Lessons Learned 25 - 27 March 2015 Geneva, Switzerland.

5 UNCTAD "Summary of adoption of e-commerce legislation worldwide". In the ECOWAS region, countries with e-transaction laws include: Benin, Burkina Faso, Cabo-Verde, Cote d'Ivore, Gambia, Ghana, Guinea, Liberia, Senegal, and Togo. Sierra Leone has no legislation while

Further to the problem of regulations, some African countries such as Nigeria have challenges such as digital divide and electronic illiteracy[6] and these challenges are epitomised by unaffordable internet access, inadequate technological infrastructure, incessant power failures, and lack of legal protection for internet-related infringements.[7]

The internet penetration rate per population in Africa is represented in a table below. From a look at the source dated 31 December 2017, Africa was populated by some 1 287 914 329 people, of this figure, there were about 453 329 534 internet users which accounted for 35.2 per cent of the African population. From an updated version of the statistics for 31 March 2020, African population is estimated at 1 340 598 447 at an internet penetration rate of 39.3 per cent of the African population. The inadequacy of infrastructural development notwithstanding, Africa accounts for at least eleven point five per cent of internet penetration in the world.[8] Also, cross-border trade in the region is very active which underlines the urgent need for the harmonisation of e-commerce regulations.

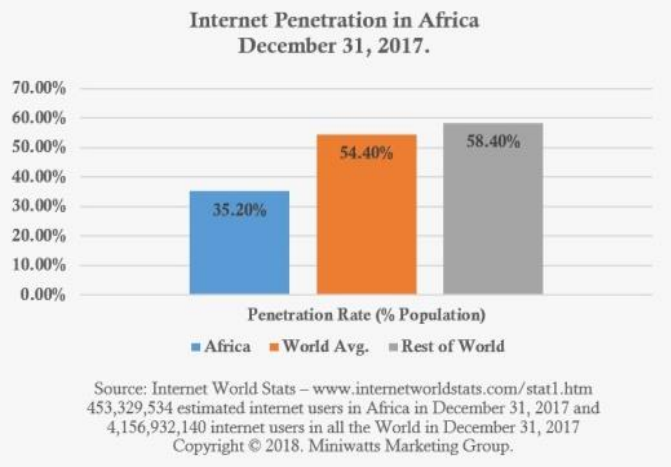
Guinea Bissau, Niger and Nigeria have draft laws, available at www.unctad.org (date of use: 03 July 2020).

6 Digital divide has been expressed to include the inequality of access to communications technology and the internet and the gap between those who have the necessary skill to use ICT infrastructures, see Ndonga (2012) 5 *African Journal of Legal Studies* 250-251.

7 Onuoha "The state of internet access" 11-16, 18.; see further the general state of infrastructure in Africa Uzoka, Shemi and Seleka (2017) 31/4 *Electronic Journal on Information Systems in Developing Countries* 1 & Ndonga (2012) 5 *African Journal of Legal Studies* 243, 251.

8 See www.internetworldstats.com (date of use: 09 September 2018); see update on "World internet usage and population statistics 2020-Q1-March-updated" at www.internetworldstats.com (date of use 20 July 2020).

Table 5.1 Internet penetration in Africa



Africa as a continent is represented by the AU. Within the AU, there are Regional Economic Communities (RECs), namely the: Southern African Development Authority (SADC); East African Community (EAC); Common Market for Eastern and Southern Africa (COMESA); Economic Community of Central African States (ECCAS); Economic Community of West African States (ECOWAS); West African Economic and Monetary Union (WAEMU); Intergovernmental Authority on Development (IGAD); Community of Sahel-Saharan States (CEN-SAD); and the Arab Maghreb Union (UMA).[9] Of note is the African Organisation for the Harmonisation of Business Law in Africa (OHADA) which is an international organisation that was created for economic integration in Africa.[10]

Convergence of ICT and e-commerce regulation in Africa is underscored by individual national legislation. In a bid to achieve harmonisation of ICT regulation in Africa, the International Telecommunications Union (ITU) and the EU signed an agreement to

9 For further information see UNECA "Regional economic communities" http://www.uneca.org/oria (date of use: 13 October 2020); UNCTAD *Review of e-commerce legislation* 3.

10 OHADA "History of OHADA" available at www.ohada.org (date of use: 15 October 2020).

establish the harmonisation of policies suitable for ICT market in Africa.[11] The project identified collective efforts undertaken in some of these regions to promote harmonisation. These efforts culminated in laws, benchmarked to international standards, to create an enabling electronic environment for consumers within and outside of Africa through the introduction and adoption of electronic legislation (e-legislation). Some of these instruments were extant, while others were in draft awaiting adoption.[12]

The following are legal instruments on consumer protection in Africa: the AU Convention on Cyber Security and Personal Data Protection (AU Convention), the SADC Model Law on Electronic Transactions and E-commerce, the EAC Framework for Cyber Laws Phase One, the COMESA Model Law on E-transactions, the ECOWAS Supplementary Act on Electronic Transactions, and aspects of the OHADA Uniform Act on General Commercial Law which regulates electronic messages and transactions. These legal instruments on consumer protection are similarly worded and modelled after the UNCITRAL Model Law and as such their legislative texts will not necessarily be outlined below except for emphasis and in areas of disparity. These legal instruments are discussed in what follows.

5.1.1 African Union

Africa's integration dates back to the establishment of the Organisation of African Unity (OAU) in 1963 when African states recognised the need to come together to achieve greater peace and unity within the region.[13] As a continental organisation, the OAU provided an effective forum which enabled all member states to adopt coordinated positions in international fora on matters of common concern to the continent, and to

11 HIPSSA-*ICT Regulatory Harmonisation: A Comparative Study of Regional Initiatives* 2009 available at www.itu.int/ITU-D/projects/ITU EC ACP/ (date of use: 14 October 2020).

12 For more information on the harmonisation process see, HIPSSA-*ICT Regulatory Harmonisation: A Comparative Study of Regional Initiatives* 2009 available at www.itu.int/ITU-D/projects/ITU EC ACP/ (date of use: 14 October 2020).

13 AU "AU in a Nutshell" available at www.au.int/en (date of use: 13 October 2020).

defend the interests of Africa effectively.[14] Until July 1999, African countries had been united in their quest for unity and economic and social development under the OAU, but at that point the Heads of Government issued a declaration (the Sirte Declaration) calling for the establishment of an African Union.[15]

In the year 2000, the Lome summit held and adopted the Constitutive Act of the African Union; it was at that summit that the AU came into being.[16] The AU is made up of 55 member states.[17] The organs of the AU include the Assembly, the Executive Council, the Commission, the Pan-African Parliament, and the Court of Justice, amongst others.[18] Cardinal among the roles of the AU is the coordination and harmonisation of its rules with those of the Regional Economic Committees (REC's) through the AU Commission.[19]

The overwhelming response of regional communities in addressing emerging trends in e-commerce, apparently to promote e-commerce and protect online users, culminated in the drafting of the AU Convention.[20] At the regional level it was clear that continent-wide consumer protection could not be achieved in the face of divergent levels of protection as harmonisation was quintessential to enforcing consumer protection across borders in internet related issues.[21]

Furthermore, in 2014 ECOWAS representatives[22] attended a workshop in which they advocated for the harmonisation of e-commerce laws in Africa.[23] At the workshop it

14 Ibid.
15 Ibid.
16 Ibid.
17 A list of the AU member countries is available at https://au.int/en/treaties (date of use: 08 October 2020).
18 Abyssinialaw "The organs of African Union" available at https://abyssinialaw.com (date of use: 28 December 2020).
19 African Peer Review Mechanism *The African Governance Report* (2019) 26 available at www.au.int (date of use: 19 July 2020).
20 Orji (2018) 12/2 *Masaryk University Journal of Law & Technology* 92, 96.
21 UNCTAD *Review of e-commerce legislation* 5.
22 ECOWAS English-speaking countries of Ghana, The Gambia, Guinea-Bissau, Liberia, Nigeria, Sierra Leone, and Cape Verde.
23 It was a four-day workshop on "Cyber Legislation in the Economic Community of West African

was recommended that: the AU Convention on Cyber Security and the Protection of Personal Data should be ratified and that legislation on consumer protection, taxation, and cross-border e-payments should be developed.[24] It was also recommended that a regulatory framework for "e–signature, electronic certification, domain name regulation, and a regional certification authority"[25] should be set up for ECOWAS countries.

In furtherance of these aims, and especially to strengthen existing legislation on ICT in member states and the RECs, on 27 June 2014 the Union adopted the AU Convention on Cyber Security and Personal Data Protection in Malabo during the 23rd ordinary session of the Assembly.[26]

5.2 AU Convention on Cyber Security and Personal Data Protection 2014

The AU Convention was adopted primarily to promote e-legislation in Africa and to fill existing gaps in regulations in the areas of: legal recognition of data communications and e-signature; intellectual property rights; personal data and information systems; e-services and telecommunication.[27] It is pertinent to state that of the 55 members of the AU, seventeen of these African countries are signatories to the UNCITRAL Model Law.[28] For the purpose of achieving some level of uniformity and certainty, it should follow that the provisions of the AU Convention and those of the UNCITRAL Model Law should be on the same level of application.

States (ECOWAS) Region" organised by the UNCTAD, the African Centre for Cyberlaw and Cybercrime Prevention, and the Council of Europe, available at www.unctad.org (date of use: 05 October 2020).

24 Ibid.

25 HIPSSA-*ICT Regulatory Harmonisation: A Comparative Study of Regional Initiatives* 2009 available at www.itu.int/ITU-D/projects/ITU EC ACP/ (date of use: 14 October 2020).

26 Samme-Nlar "Why it is important for African States to ratify the Malabo Convention" available at https://www.aanoip.org (date of use: 29 October 2020); see also UNCTAD *Review of e-commerce legislation 3;* Amazouz "African Union perspectives on cybersecurity and cybercrime" 5; Tarmakin "The AU's cybercrime response" 3.

27 See the preamble to the AU Convention on Cyber Security and Personal Data Protection adopted on 27 June 2014 in Malabo during the 23rd ordinary session of the Assembly.

28 These are the African countries that have signed the UNCITRAL Model Law and have enacted laws influenced by the Model Law, Botswana; Cape Verde; Gambia; Ghana; Liberia; Madagascar; Malawi; Mauritius; Mozambique; Rwanda; Seychelles; Sierra Leone; South Africa; Tanzania; Togo; Uganda; and Zambia, see UNCITRAL "UNCITRAL Model Law on Electronic Commerce (1996) – Status" available at www.uncitral.org (Date of use: 28 October 2020).

5.2.1 Provisions

The AU Convention is an all-embracing instrument providing for e-transactions, data protection, and cyber security. Chapter 1 of the Convention containing articles 1-7, covers a large area of e-transactions and applies to both B2B and B2C transactions. Chapter 2 of the AU Convention applies to personal data protection; Chapter 3 provides for the promotion of cyber security and combating of cybercrime; while Chapter 4 embodies the final provisions.[29]

The AU Convention applies to e-commerce activities[30] and provides for e-signatures; e-payments; and e-contracts where the parties elect to use electronic means.[31] Consumers are to be provided easy, direct, and uninterrupted access to e-communications by ISPs and online merchants.[32] As with some documents on e-transactions, article 1 of the AU Convention defines data-related terms but fails to define a consumer.

Six basic principles are established in the AU Convention.

(a) Principle governing information requirements

In article 2(2) of the AU Convention the principle on rules on information requirements is established and provides that state parties shall ensure that any person exercising e-commerce activities provides the following information where applicable.

(i) The name of the individual involved, or if it is a legal person, its business name and address, registration, and contact details, as well as licensing information and applicable rules.

(ii) The tax identification number.

---

29 The parts of the Convention are itemised in Amazouz "African Union perspectives on cyber security and cybercrime" 7.

30 AU Convention on Cyber security and Personal Data Protection,adopted on 27 June 2014 in Malabo during the 23rd ordinary session of the Assembly see arts 2(1) and 5(5).

31 AU Convention arts 5(1) and 6(2).

32 AU Convention art 2(2).

(iii) Price, taxes, delivery, and other charges.

(b) Principle governing jurisdiction

There is no harmonised convention or regulation in Africa on jurisdiction or on the recognition and enforcement of judgments in civil and commercial matters as one finds in the EU. Therefore, applying harmonised rules on consumer protection would necessitate continent-wide rules on jurisdiction. In recognition of this, the AU Convention provides that the activities of a provider or business are subject to the law of the state party in whose territory the provider is established, unless otherwise agreed by the parties. This position aligns with the standard rules on jurisdiction applied within the EU.[33]

(c) Principle governing commercial communications

E-commerce activities are generally initiated by promotional offers and advertisements. However, problems arise where commercial communications constitutes spam which impacts negatively on the right to privacy.[34] Consequently, direct marketing and the sale of unsolicited goods are expressly prohibited in certain jurisdictions.[35] Under the AU Convention,[36] direct marketing is prohibited unless the prior consent of the recipient has been obtained, and must thereafter include easy and cost-free opt-out provisions. The AU Convention favours the opt-in model in terms of which direct marketing is not allowed without the recipient's prior consent. There is no consensus on an international model governing unsolicited communications. Some jurisdictions favour the opt-in model which requires prior consent,[37] while others favour the opt-out model where the requirement of prior consent is dispensed with and suppliers need only provide an easy, timeous, and cost-free opt-out provision.[38]

---

33 Compare art 3 of the AU Convention with art 3(1) of the E-commerce Directive.

34 Tladi *The South African Law Journal* (2008) 125/1 183; see also Michalsons "The law vs unso licited commercial communications" 2003 available at www.michalsons.com (date of use: 30 October 2020).

35 See, for example, the EU under the provisions of the Privacy and Electronic Communications Directive 2002 and the Canadian Anti-spam legislation, 2014.

36 AU Convention art 4(3) and (5).

37 EU under art 13 of the Privacy and Electronic Communications Directive.

38 The opt-out model is obtainable in South Africa under s 45 of the ECTA.

All marketing communications must be clearly identified and should disclose the individual or corporate body on whose behalf they have been disseminated.[39] Concealing the identity of a person on whose behalf an advertisement is issued is prohibited.[40] The AU Convention further provides that in the case of promotional offers, the conditions for participation must be spelt out and easily accessible.[41] Although a debate on the Convention advocates that the provision of this article should go beyond marketing communications to all forms of unsolicited mails.[42]

(d) Principle governing electronic contracts

The use of electronic means for contract formation is acceptable unless the parties to the transaction have agreed otherwise before the conclusion of the contract.[43] In order to accord legal recognition to e-transactions, in article 5 of the Convention the following safeguards are provided:

(i) Contracts should be processed in a durable medium that is capable of being accessed and reproduced.

(ii) The recipient should have the opportunity to verify his or her details, and especially the price of the goods before confirming the order.

(iii) The provider shall acknowledge receipt of the confirmation without delay and by electronic means.

(iv) The receipt of any of the information of offer and acceptance shall be deemed to have been received when the parties to whom it is addressed are able to access it.[44]

The implication of the safeguard in article 5(4) of the AU Convention is that where the addressee, for example, is unable to access the communication due to hardware

39 AU Convention art 4(1).
40 AU Convention art 4(6).
41 AU Convention art 4(2).
42 Githaiga *A report of the online debate* 7.
43 AU Convention art 5(1).
44 AU Convention art 5(4).

malfunction, infrastructural failure, ineptitude, or negligence, the communication will not be deemed to have been received, irrespective of the fact that, in the case of an e-mail, the communication has left the information system of the originator for that of the addressee. For web pages, too, there must be an act indicating acknowledgement of receipt in order to qualify under the paragraph. The challenge with this safeguard is that for e-mails it is impracticable to show that the communication has actually been accessed by the addressee unless evidence is called to show whether or not a specific communication was actually accessed. National laws must, therefore, provide a procedural step which consumers must follow to show "receipt", failing which the communication is deemed to have been inconclusive. Under the AU Convention, the delivery of e-communications is only effective once the addressee or supplier acknowledges receipt; more of an adaptation of the information theory.[45]

An alternative to the requirement of acknowledgement includes a proposal by, Gringas and Nabarro[46] that e-mail offers should be subject to a date on which the offer will lapse. An objective date and time should be specified, that way, if no intention is shown during the lifespan of the offer, the offer would naturally elapse. The crux of the matter is whether the mere fact that a communication has been sent is sufficient to impose obligations. Article five of the AU Convention however, disposes of this alternative by requiring the use of an acknowledgement as a condition for proof of receipt. The aim of this is that an acknowledgement by the parties will exclude any technical or legal issues that may be associated with proof of receipt.

While the above provision appears cumbersome, it affords the consumer greater protection in that he or she is able to review an order and have it confirmed and

---

45 The information theory requires that the receipt of an offer is brought to the knowledge of the offeror before becoming effective. This theory is unlike the receipt theory that concludes communication once it is shown that a message has left the information system of that of the originator to the recipient where it is capable of being retrieved. The receipt theory is more founded in most e-commerce laws especially those which are modeled after the UNCITRAL Model Law, see Cupido "Offer and acceptance in cross-border electronic contracts: A brief comparative perspective" 2015 5 available at www.ase-scoop.org (date of use: 05 September 2020).

46 Gringas & Nabarro *Laws of the Internet* 16.

acknowledged by the supplier. The communication process is transparent and is capable of terminating the contract mid-way in the absence of an acknowledgement of receipt. The requirement of acknowledgement of receipt however, can be waived by agreement between businesses (B2B).[47]

(e) Principle governing validity of electronic communication

The AU Convention does not require communications to be by electronic means, but where writing is a requirement, that requirement is met through the functional equivalence of a data message.[48] E-communications are also subject to specific conditions of legibility and reproduction, where their paper equivalent so demands.[49] E-communications are admissible in evidence in the same way as paper-based documents,[50] provided that, the originator can be duly identified and the communication has been completed and retained in a manner that guarantees its integrity.

(f) Principle governing security of electronic transactions

E-payments must be made using methods approved by the parties with the onus resting on the supplier to show that all necessary obligations have been discharged, or that they did not exist.[51] Certified true copies of a copy of an electronically signed contract shall have the same probative value as the contract itself.[52]

The AU Convention is open to all member states of the Union for signature, ratification, or accession.[53] Provision is also made for state parties to submit proposals for the

47 UNCITRAL Model Law art 5(5).
48 AU Convention art 6(2).
49 AU Convention art 6(1).
50 AU Convention art 7(3).
51 AU Convention art 7(1).
52 "An electronic signature is created by a secure device which the signatory is able to keep under his exclusive control and is appended to a digital certificate shall be admissible as signature on the same terms as a handwritten signature." See AU Convention art 7(4).
53 See art 35 of the AU Convention. The Convention has been ratified by five countries and they are Ghana, Guinea, Mauritius, Namibia and Senegal. A total of 14 countries have, however, signed the Convention, available at http://au.int/en/treaties (date of use: 08 October 2020).

amendment or revision of the AU Convention. State parties may also enter reservations to the AU Convention or withdraw totally from it.[54]

5.2.1.1 Exclusions

In terms of article 2(1), the AU Convention does not apply to gambling or acts requiring legal representation, including activities performed by notaries or equivalent authorities. In the context of contracts, the AU Convention does not permit e-communications in respect of the following:

(i) wills, signed private family deeds; and
(ii) private acts, whether civil or commercial, except in respect of a professional purpose.[55]

5.2.2 Limitations

The AU Convention was adopted in the wake of new technologies in e-communications yet it does not reflect improvement in terms of technology. The protection of the peculiar needs of e-mobile consumers is not addressed neither is there any provision to protect minors who go online to transact.

The information requirements are not sufficiently comprehensive to cater for the challenges which consumers may face when shopping online. There are no safeguards for consumers who may wish to withdraw from a contact due to the inability of suppliers to provide vital information. In addition, although the AU Convention provides for the validity of e-communications, it fails to refer to the legal approach of member states to automated transactions.

54 AU Convention art 38(2).
55 AU Convention art 6(3).

A further limitation is that the elaborate provision for a confirmation process notwithstanding, there is no provision for refunds where necessary. The AU Convention does not provide for incorporation by reference, neither is there a regulation governing unfair terms or the prohibition of sales of unsolicited items. Consumers' payment systems are provided but not protected in the AU Convention. Although reference is made to dispute resolution, the provision is very basic and unconvincing and it fails to establish an enforcement agency to deal with consumer transactions.[56]

Unfortunately, there are no specific procedural rules for the discharge of the obligations of suppliers to consumers which would allow for uniform regulations addressing liabilities, time for performance, or cancellation in the event of non-performance. When it comes to e-contracts, the AU Convention makes no provision for pre-offers or place of dispatch and receipt. These *lacunae* create room for national legislatures to enact disparate rules to fill the gaps. This, of course, erodes the objective of harmonisation.

5.2.3 Enforcement and implementation of the AU Convention

The AU Convention has no laid-out structure for enforcing consumer protection principles. There are however, attempts to encourage mutual sharing and understanding through the submission of regular reports to the Executive Council of the African Union on the progress made by each state party, but without specific time frames.[57] Should disputes arise from the implementation and enforcement of the AU Convention, such disputes shall be settled amicably through direct negotiations between the state parties concerned, and where direct negotiation fails; disputes may be resolved through any ADR mechanism.[58]

---

56 See Githaiaga *A report of the online debate* 22 on the weak provisions of the Convention on implementation.

57 AU Convention art 32.

58 AU Convention art 34.

5.3 Consumer Protection in Southern and Eastern Africa

Southern Africa operates through the SADC, while East Africa falls under the auspices of the EAC. Together they carry out their economic activities under the COMESA by virtue of the 1992 COMESA treaty. The backgrounds to these regions and their instruments on consumer protection are briefly considered and the COMESA dispute resolution system is discussed in what follows.

5.3.1 Southern African Development Community

The SADC is a regional community made up of sixteen countries in the Southern part of Africa.[59] The SADC was previously the Southern African Development Coordinating Conference (SADCC) which was established on 1 April 1980, but was transformed into the SADC by the adoption of the SADC treaty on 17 August 1992 in Windhoek, Namibia.[60] Through the treaty, the basis of cooperation among member states was redefined from a loose association into a legally binding arrangement. Consequently, the SADC protocols and decisions are legally binding documents for member states.[61] The objectives of the SADC are to achieve developmental peace and security, promote economic growth to alleviate poverty, enhance the standard and quality of life of the peoples of Southern Africa, and support the socially disadvantaged through regional integration, built on democratic principles and equitable and sustainable development. The organisation has a total of fifteen member states all of whom are also members of the AU. The SADC is part of the tripartite cooperation between the EAC and the COMESA. However, not all members of the SADC are members of the COMESA.[62]

---

59 These countries are Angola; Botswana; Comoros; Congo Dem Rep; Eswatini; Lesotho; Madagascar; Malawi; Mauritius; Mozambique; Namibia; Seychelles; South Africa; Tanzania; Zambia and Zimbabwe see SADC "About SADC" available at www.sadc.int (date of use: 20 October 2020).

60 SADC "Southern African Development Community (SADC)" available at www.au.int (date of use: 26 July 2020).

61 Ibid.

62 South Africa, Angola, Botswana, Lesotho, Mozambique, Namibia, and Tanzania are not members of COMESA. COMESA member states are Burundi; Comoros; Congo Dem Rep; Djibouti;

5.3.2 SADC Model Law on Electronic Transactions and Electronic Commerce 2012

The SADC came up with the proposal for a Model Law in 2012 following the trend in e-commerce applications and the need for harmonised rules on consumer protection and internet trade with the cooperation of the International Telecommunications Union (ITU).[63] The SADC Model Law on Electronic Transactions and E-commerce (the SADC Model Law) provides a tool that member states can use to create a more secure legal environment for e-transactions and e-commerce. It seeks to enhance regional integration using the best practices and collective efforts of member states to address legal aspects of e-transaction and e-commerce. Quite unlike the AU Convention, the SADC Model Law does not contain comprehensive regulations on data protection; these are rather contained in a different piece of legislation known as the SADC Model Law on Data Protection[64].

5.3.2.1 Provisions

The SADC Model Law is technologically neutral[65] and captures the essential principles on consumer protection which include: the validity of e-communications;[66] recognition of e-contracts and automated transactions;[67] incorporation by reference and party autonomy.[68] While the Model Law provides functional equivalence for e-communications by requiring that where writing is required by law, data fulfils that

Egypt; Eritrea; Eswatini; Ethiopia; Kenya; Libya; Madagascar; Malawi; Mauritius; Rwanda; Seychelles; Somalia; Sudan; Tunisia; Uganda; Zambia and Zimbabwe see COMESA "Member States" available at https://comesa.int (date of use: 26 June 2020)

63 SADC Model Law, preamble available at https://www.itu.int/electronic transaction (date of use: 05 October 2020).

64 SADC Model Law on Data Protection 2012.

65 The Model Law is said to be technologically neutral since it can be applied to existing as well as future technologies, see para 5 of the Preamble to the SADC Model Law.

66 SADC Model Law s 4 and reflects the same position under the UNCITRAL Model Law art 11.

67 See ss 10 & 16 SADC Model Law; see also arts 5 & 13 of the UNCITRAL Model Law.

68 SADC Model Law ss 9 and 11; see further arts 5*bis* & 4 of the UNCITRAL Model Law.

function provided it is available for future reference.[69] Similarly, e-signatures are valid when applied within the scope of the SADC Model Law.[70] With the use of data messages, contracts enjoy full legality and can be adduced as evidence in any court of law or tribunal.[71] It is noteworthy that very much like the provisions of the UNCITRAL Model Law in its art 15; the SADC Model Law clearly indicates rules on the determination of the time and place of dispatch and receipt of e-communications.[72] Under the SADC region, the use of direct commercial communications or advertisements which are directly targeted at recipients are not expressly prohibited. However, the privacy of e-commerce consumers is protected through rules on direct commercial communications.[73] Vendors or service providers are permitted to send commercial communications to recipients on the following conditions where: there is sufficient information to identify the sender; there is a valid opt-out facility and where the sender discloses the source where the personal information of the recipient was obtained. The privilege to send direct commercial communications to recipients is effectively protected through additional safeguards in the law and a breach of these safeguards could attract fines or imprisonment not exceeding five years.[74]

In examining the SADC Model Law it is safe to state that the Model Law sufficiently implements the provisions of the UNCITRAL Model Law based on the above principles. The SADC Model Law improves on the scope of the UNCITRAL Model Law by incorporating rules on the limitation on the liabilities of service providers into its provisions to meet up with the EU standard as contained in the E-commerce Directive..[75] Further included in the SADC Model Law are consumer protection rights that are peculiar to online users and these are the rights of consumers to information, confirmation, performance, cooling-off, withdrawal, and refunds.[76]

---

69 SADC Model Law s 6, similarly provided in art 6 of the UNCITRAL Model Law.
70 SADC Model Law s 7; see also art 7 of the UNCITRAL Model Law.
71 See SADC Model Law ss 10 & 20 as a reflection of what obtains under the UN Model in art 9 of the UNCITRAL Model Law.
72 SADC Model Law ss 13 and 14.
73 SADC Model Law s 30.
74 SADC Model Law s 30(8).
75 See SADC Model Law ss 31-34 and compare with arts 12-15 of the E-commerce Directive.
76 These rights are contained in ss 25-27 of the SADC Model Law and more particularly contained

An innovation in the SADC Model Law is its procedural requirement for the deposition of an affidavit in tendering e-communications made in the ordinary course of a business.[77] The Model Law also lays down procedures for take-down notices should the need arise.[78]

5.3.2.2 Exclusions

The SADC Model Law applies to B2C transactions but does not apply the principle of functional equivalence of writing and signature to a contract for the alienation of immovable property; long-term lease of immovable property which exceeds twenty years; the execution, retention, and presentation of a will or codicil; the execution of a bill of exchange; and such other documents or instruments as may be prescribed by member states.[79]

The SADC Model Law does also not allow the exercise of the right of withdrawal in respect of: financial services; auctions; supply of foodstuff; services that began with the consumer's consent within a cooling-off period; the supply of services dependent on fluctuations; goods made to the specification of the consumer or personalised goods; goods that cannot by their nature be returned, or goods that deteriorate or expire rapidly; the supply of audio or video recordings or computer software that have been unsealed by the consumer; the supply for sale of newspapers, periodicals, magazines, and books; the provision of gaming and lottery services; online gambling; accommodation; transport; catering; and other exceptions which member states may find necessary.[80]

---

in arts 6, 8-15 of the European CRD.

77 SADC Model Law s 20(4).

78 SADC Model Law s 35.

79 SADC Model Law ss 6-7.

80 SADC Model Law s 27.

5.3.2.3 Limitations

There are no provisions on jurisdiction; information on operability of digital products; dispute resolution; protection for mobile consumers (m-consumers) or minors; or enforcement and implementation agencies.

5.3.2.4 Summary

The SADC member states are also members of the AU which should provide a wider coverage for its members. The harmonisation of law in the Southern African region should, therefore, reflect the principles in the AU Cyber-security Convention and the principles contained in the UNCITRAL Model Law. The first steps towards achieving this should be the adoption of the AU Convention and the UNCITRAL Model Law by the SADC States. In this regard five of the SADC states have signed the AU Convention[81] while eight states are signatories to the UNCITRAL Model Law.[82] There is therefore an apparent gap within the region on the unification of e-commerce and e-commerce consumer protection laws. However, this study has shown that the SADC Model Law provides wider consumer protection measures than the AU Convention. There is, however, an area in which the two instruments do not synergise, namely, the rules governing unsolicited commercial communications. While the AU Convention expressly prohibits direct commercial communication, the SADC states are allowed to permit such communications provided recipients are able to opt out freely and easily. It will be observed that the SADC Model Law is more in tune with international standards on consumer protection when its sections 12 and 14 are compared with article 15 of the UNCITRAL Model Law, or when the SADC Model Law's sections 31-34 are compared with articles 12-13 of the E-commerce Directive. Overall, the protection

81 These states are Comoros, Congo Democratic Republic; Rwanda, Tunisia and Zambia, see AU "List of countries which have signed, ratified/acceded to the African Union Convention on Cyber Security and Personal Data Protection" available at http://au.int (date of use: 20 October 2020).

82 Botswana, Madagascar, Malawi, Mauritius, Mozambique, Seychelles, South Africa and Tanzania are the SADC member states that have signed the UNCITRAL Model Law see UNCITRAL "UNCITRAL Model Law on Electronic Commerce (1996) – status" available at www.uncitral.org (date of use: 28 October 2020).

afforded by the SADC Model Law is an improvement on the AU Convention and re-enforces the need for greater collaboration in the harmonisation of e-commerce protection principles in Africa.

5.3.3 East African Community

The EAC is a regional intergovernmental organisation comprising of the Republics of Burundi, Kenya, Rwanda, South Sudan, the United Republic of Tanzania, and the Republic of Uganda; headquartered in Arusha, Tanzania. Member states of the EAC are also members of the AU and, with the exceptions of South Sudan and Tanzania, are also members of the COMESA.[83] The treaty establishing the EAC was signed on 30 November 1999 and entered into force on 7 July 2000 following its ratification by the three original partner states: Kenya, Uganda, and Tanzania. The Republic of Burundi and Rwanda acceded to the treaty on 18 June 2007, and became full members of the community as from 1 July 2007.[84] Under article 3 of the treaty, the partner states may, upon such terms as they determine, negotiate with any foreign country or association on granting of membership. The objectives of the community are to develop policies and programmes aimed at widening and deepening cooperation among the partner states in the political, economic, social, and cultural fields, and on research and technology, defence, security, legal and judicial affairs, for their mutual benefit.[85]

In pursuance of these objectives, a common market was established by the partner states for the acceleration, and sustained expansion of economic activities within the community in order to achieve a harmonious and balanced development.[86] To this end,

---

83 EAC "Overview of EAC – East African Community" available at www.eac.int (date of use: 26 October 2020); see also COMESA "COMESA members states" available www.comesa.int/comesa-members-state (date of use: 26 October 2020).

84 EAC "Overview of EAC – East African Community" available at www.eac.int (date of use: 26 October 2020).

85 EAC Treaty art 5.

86 MEAC "Common Market" available at www.meac.go.ke/commonmarket (date of use: 05 July 2020).

in November 2006, the EAC Council of Ministers adopted the EAC Strategy for E-Government, which included a recommendation to develop a legal framework for cyber laws.[87] In December 2007, the EAC partners' states appointed a Task Force on Cyberlaws comprising representatives from the partner states and the EAC Secretariat with the support of UNCTAD.[88]

The Task Force recommended that the framework be prepared in two phases and that the process of law reform be coordinated at a regional level and harmonised and benchmarked against international best practice.[89] Framework 1 addresses five key issues on e-transactions; e-signatures and certification services; data protection and privacy; consumer protection; and computer crime.[90] Framework II complements the framework prepared in Phase 1, and focuses on issues of intellectual property; competition; taxation; and information security.[91] For the purpose of this study Framework I only, will be discussed.

5.3.4 Framework for Cyber Laws: Phase 1, 2008

The framework for cyber laws was based on a series of recommendations made to the governments of the partner states to reform national laws to facilitate e-commerce and the use of data security mechanisms.[92] The recommendations for the framework aimed at protecting privacy, use of e-communications and the promotion of e-commerce.[93] The framework was adopted at the 2nd Extraordinary Meeting of the EAC Sectorial Council on Transport and Meteorology in May 2010.[94]

87 Batuwa "Development and implementation" 11.
88 UNCTAD "East African Community" (2007) available at http://unctad.org (date of use: 05 July 2020).
89 UNCTAD *Harmonising cyberlaws and Regulations* 7.
90 GTAD "Meeting of the East African Community (EAC) Task Force on Cyberlaws" available at www.gtad.wto.org (date of use: 30 November 2020).
91 Ibid.
92 UNCTAD *Harmonising cyberlaws and Regulations* 6.
93 Executive summary, Draft EAC Legal Framework for Cyber Laws November 2008.
94 Executive summary, Draft Framework for Cyber Laws Phase II February 2011, 2.

The framework implements the provisions of the EC Convention,[95] and extends its scope of application to B2C contracts. It attempts to harmonise e-commerce and consumer protection rules with the UNCITRAL Model Law on E-Commerce and the Commonwealth Model Law on Electronic Transaction, 2002.[96] What the EAC seeks to achieve by the adoption of a framework for cyber law is to facilitate domestic and international e-commerce by eliminating legal barriers, establishing legal certainty, and encouraging the use of reliable forms of e-commerce.[97] It also seeks to facilitate electronic filling of documents with government services by means of reliable forms of e-communication, and to promote public confidence in the authenticity, integrity, and reliability of data massages and e-communications.[98]

5.3.4.1 Provisions

The framework applies to e-transactions which include agreements for the purchase of goods, products, or services. It also applies to interaction with government and administrative bodies in either a commercial or non-commercial context.[99] It embodies generally established principles of e-commerce and consumer protection such as: party autonomy;[100] terms incorporated by reference;[101] technological neutrality;[102] validity of e-communications;[103] contract formation and use of automated systems;[104] record-keeping and evidentiary requirements.[105] The EAC Framework clarifies issues on time and place of dispatch of e-communications;[106] the use and acceptance of

95 The EAC Task Force recommends that the Cyber Law Framework reflects international stand ards. These are implemented in rules 5 (recognition of e-data), 6 (incorporation of terms in contract), and 9 (rules on time and place of dispatch and receipt of e-communications). These rules are expected to be couched in the same wording as that used in the EC Convention.
96 Draft EAC Legal Framework for Cyber Laws November 2008, 4.
97 UNCTAD *Harmonising cyberlaws and Regulations* 6.
98 EAC Framework Phase 1, rule 1.
99 EAC Framework Phase 1, rule 2.
100 EAC Framework Phase 1, rule 3.
101 EAC Framework Phase 1, rule 6.
102 EAC Framework Phase 1, rule 14.
103 EAC Framework Phase 1 rule 5.
104 Ibid.
105 EAC Framework Phase 1, rule 7.
106 EAC Framework Phase 1, rule 9.

electronic modes of communication by public authorities;[107] limited liability of ISPs for third-party content and provision for the removal of illegal content.[108] The framework further makes provision for consumers right to information;[109] cancellation within a specified timeframe;[110] a secured payment system;[111] as well as performance.[112]

5.3.4.2 Exclusions

The law applies to civil and administrative communications as well as contracts, but does not apply to criminal matters or criminal procedure.[113]

5.3.4.3 Limitations

Gaps in the framework are observed in the information requirements which do not appear to take cognisance of the role of professional bodies by requiring that information on such bodies is displayed. As with most other regulations, there is no provision for the protection of consumers of digital products and m-commerce. Again, the framework does not address the issue of spam and inertia selling.

5.3.4.4 Summary

The EAC Framework for Cyber Laws is consistent with the provisions of the UNCITRAL Model Law thus signifying a unification of purpose and a reflection of international standards. Though the EAC Framework builds significantly on the UNCITRAL Model Law and the AU Convention, ratification of the Convention and of the Model Law has been poor within the region, for instance it is only Tanzania among

107 EAC Framework Phase 1, rule 10.
108 EAC Framework Phase 1, rule 11.
109 EAC Framework Phase 1, rule 18.
110 Ibid.
111 Ibid.
112 Ibid.
113 EAC Framework Phase 1, rule 2.

the EAC member states that has signed the UNCITRAL Model Law.[114] Similarly, it is only the state of Rwanda among the EAC member states that has signed the AU Convention.[115] Nonetheless, the provisions of the Framework for Cyber Law Phase 1 are quite comprehensive save for a few gaps as listed in the paragraph above.[116] These gaps notwithstanding, the recommendation by the Task Force on implementation is commendable, and would result in a sustainable cyber protection era if properly followed. The Sectorial Council of the EAC has urged partner states to adopt and implement the recommendations of the Task Force, and has directed the EAC Secretariat to monitor and give report on its implementation.[117] The Task Force also recommends that partner states set up their own institutions for the regulation of the framework.[118]

5.4 Common Market for Eastern and Southern Africa

The COMESA is a common market for Eastern and Southern Africa established by the heads of government of 21 states[119] under the COMESA Treaty to replace the former Preferential Trade Area (PTA) for Eastern and Southern African states which had existed since 1981.[120] Cardinal among the objectives of the market is to cooperate in strengthening the relations between the common market and the rest of the world.[121] The organs of the common market are the: Authority Council; Court of Justice;

114 UNCITRAL "UNCITRAL Model Law on Electronic Commerce (1996) – status" available at www.uncitral.org (date of use: 28 October 2020).

115 AU "List of countries which have signed, ratified/acceded to the African Union Convention on Cyber Security and Personal Data Protection" available at http://au.int (date of use: 20 October 2020).

116 See para 5.3.4.3 above.

117 Kenya, Rwanda and Uganda have enacted legislation on Electronic transactions and Signatures see UNCTAD *Harmonising cyberlaws and Regulations* 2013 7; Burundi has a draft law on Electronic transaction while Tanzania has an Electronic transaction law see UNCTAD "E-transactions legislation worldwide" available at https://unctad.org (date of use: 30 November 2020).

118 Ibid.

119 COMESA *COMESA in brief* 2018 available at https://www.comesa.int/pdf (date of use: 26 July 2020).

120 COMESA "Overview of COMESA" available at https://www.comesa.int (date of use: 26 August 2020).

121 COMESA Treaty art 3(e).

Committee of Governors of Central Banks, Intergovernmental Committee; Technical Committee; Secretariat; and Consultative Committee.[122] The directions and decisions of the Authority Council are binding on member states and on all the other organs of the common market.[123] The EAC, the SADC and the COMESA exist under a tripartite institutional framework under which a Memorandum of Understanding was signed to underpin the legal and institutional framework and to establish a tripartite coordination mechanism.[124]

Regulations on consumer protection have been approached from the perspectives of the EAC and SADC regional organisations. It may, therefore, not be of much practical value to undertake a detailed discussion of the COMESA Model Law on e-transactions. However, this Model Law offers an interesting insight into a well set-out dispute resolution system for online trade. Consequently, without a discussion of the Chapter Four of the COMESA Model Law on e-transactions which deals with dispute resolution, this study would be incomplete.

5.4.1 COMESA Model Law on Electronic Transactions 2010

The COMESA Model Law was drafted on the basis of the EC Convention and the UNCITRAL Model Law, to reflect international thinking on harmonised rules for e-transactions. Member states are urged by the Council of Ministers to accede to the EC Convention and to incorporate its provisions into their respective national laws.[125]

5.4.1.1 Provisions

The COMESA Model Law is divided into six chapters. Of these, Chapters 1-3 are on all fours with the provisions of the EC Convention and the UNCITRAL Model Law with

122 UNECA COMESA – "Common Market for Eastern and Southern Market" available at www.unec.org (date of use: 30 November 2020).
123 Verhaeghe & Woolfrey "Understanding COMESA and the East African power pool" 4.
124 SADC "Tripartite Cooperation" available at www.sadc.int (date of use: 26 August 2020).
125 COMESA Model Law Executive Summary 2010 at 1.

verbatim reproduction of most of their provisions except that the COMESA Model Law applies to both B2B and B2C transactions.[126] Consumer protection principles contained in the COMESA Model Law do not however, apply to e-transactions involving "financial services; auctions; supply of consumables; personalised goods; services which began with the consumer's consent; the provision of accommodation, transport, catering, or leisure".[127] They do not also apply to the sale of newspapers and periodicals; unsealed software; gaming or lottery services.[128] The COMESA Model Law improves on the UNITRAL Model Law and the EC Convention by the inclusion of consumer rights – most notably the right of withdrawal and the right to receive a refund,[129] as well as the right to review a transaction before confirmation.[130]

The information requirements in the COMESA Model Law are very comprehensive and the law actually protects consumers against non-performance.[131] However, there are no rules on applicable law or jurisdiction and there is no provision protecting ISPs from liability for third-party content. These shortcomings notwithstanding, the law is on par with other regional laws in terms of consumer protection and most of its provisions reflect international standards in line with the provisions of the EC Convention. Again, meaningful innovations are introduced in the COMESA Model Law dealing with the application of sanctions where necessary, and the innovative provisions in its Chapter 4 on, online dispute resolution.[132]

126 Ibid at Chapter 2 para C(21). Under this paragraph COMESA countries were advised by the Council to adopt the EC Convention without making an art 19 declaration which has the effect of limiting the scope of application of the COMESA Model Law. Although art 1(2) of the Law leaves room for exclusion, member states are in Chapter 5 which is a guide to the enactment – urged in para 1(B)(9) not to enact substantial restrictions so that the Law can serve its widest possible application.

127 COMESA Model Law art 22.

128 Ibid.

129 COMESA Model Law art 24.

130 COMESA Model Law art 23(2).

131 COMESA Model Law art 28.

132 Article 30 of the COMESA Model Law institutes the Court of Justice of the Common Market.

5.4.2. Online Dispute Resolution

Most consumers' fears when conducting electronic trade, center on the difficulty of resolving disputes which may arise in the event of fraud, defective products, and non-performance. Consumer purchases generally involve small sums of money; therefore, an effective redress procedure should be commensurate with the amount involved in the transaction. Such minimum cost should certainly not involve travelling, accommodation, high costs of litigation, and the instruction of counsel. Logically, since the transaction was concluded online, it is only fair that redress can also be accessed online. This latter position is what the COMESA Model Law offers in its conciliation proceedings before the Court of Justice of the Common Market. The court is open to any dispute referred to it by a party whose transaction is subject to the EC Convention or an enactment by a member state based on the COMESA Model Law.[133] The Model Law provides a guide for conciliation proceedings. It is of note that "any settlement or agreement reached between parties under the conciliation proceedings is final and binding and may be made an order of court."[134]

The conciliation proceedings must be conducted by electronic means[135] and may not be combined with other legal or arbitral proceedings until those proceedings have been concluded or the parties have withdrawn from the conciliation process.[136] Any party is entitled to withdraw from or terminate the conciliation process at any time, provided that the other party and the Registrar of Court are informed electronically.[137] Where, however, a party's right needs to be preserved, judicial or arbitral proceedings are permitted.[138] Communications in the proceedings are confidential and cannot be

133 The COMESA Treaty (art 28) was amended to expand the jurisdiction of the COMESA Court of Justice to act as conciliator in any dispute referred to it by a party whose transaction is subject to the United Nations Convention on E-communications, or to an enactment by a member state based on the COMESA Model Law.

134 COMESA Model Law art 30(7).

135 Ibid.

136 COMESA Model Law art 30(6).

137 COMESA Model Law art 30(5).

138 COMESA Model Law art 30(6).

used in a different proceeding.[139] The conciliator may not act as a witness in any subsequent proceedings, nor can a court or tribunal order the disclosure of any of the information used, expressed, or proposed during the conciliation proceedings, in subsequent proceedings.[140] However, evidence tendered in the Conciliation Court may be tendered in different proceedings.[141]

The innovation of the COMESA in establishing the Court of Justice for the Common Market serves as a lesson for all. The establishment of a common court can be an international standard which will ensure that consumer protection becomes a reality rather than a myth – especially in jurisdictions with inadequate enforcement mechanisms.

5.5 Economic Community of West African States

ECOWAS was created on 28 May 1975[142] for the economic progress of its members. The initial multilateral treaty in the region

> …was signed by the Heads of State and Governments of the then sixteen member states in 1975 in Lagos, Nigeria. With new developments and mandates for the Community, a revised treaty was signed in Cotonou, Benin Republic, in July 1993 by the Heads of State and Governments of the now fifteen member states.[143]

By signing the revised treaty, member states reaffirmed the Treaty establishing the Economic Community of West African States and their commitment to pursue interstate economic and political growth. The Commission adopts Conventions and Protocols followed by Supplementary Acts which are binding on member states.[144]

---

139 COMESA Model Law art 30(8).

140 COMESA Model Law art 30(10).

141 COMESA Model Law art 30(14).

142 Alkali "West Africa: ECOWAS-Its Formation and Achievements" *AllAfrica* 2008 available at www.allafrica.com (date of use: 22 August 2020).

143 Economic Community of West African States Revised Treaty (ECOWAS Revised Treaty). The ECOWAS countries are Benin, Burkina Faso, Cabo Verde, Cote d'Ivore, The Gambia, Ghana, Guinea, Guinea-Bissau, Liberia, Mali, Niger, Nigeria, Senegal, Sierra Leone, and Togo, available at www.ecowas.int (date of use: 22 August 2020).

144 ECOWAS "Official Journal-Supplementary Acts/Protocols/Decisions/ New Regime for Community Acts" available at www.ecowas.int/ecowas-law (date of use: 14 August 2020).

Given the revolutionary trend in the use of mobile devices, and the menace of cybercrimes in the region, it became imperative for African leaders to develop legal rules for the conduct of activities online. It was recommended that a framework for e-commerce in ECOWAS be established, with regional and global compatibility as a significant objective – particularly in view of the role of international cooperation in setting rules for technology and cross-border commerce.[145]

In the ECOWAS region, ten countries have specific e-transaction laws; four countries have draft legislation while one country has no legislation at all.[146] In order to promote uniformity in national laws within the ECOWAS region rather than disparate laws which could only amount to "re-inventing the wheel,"[147] a Supplementary Act on Electronic Transactions was adopted.[148] The Supplementary Act on Electronic Transactions in the ECOWAS Area (ECOWAS E-transactions Act) is binding on signatory states[149] and subject only to national ratification.

5.5.1 Supplementary Act on Electronic Transactions in the ECOWAS Area 2010

The ECOWAS E-transactions Act was adopted by the Authority of the Heads of States in 2010 at its 63rd meeting in November 2009 held at Abuja, Nigeria. The purpose and objectives of the Act are: to remove impediments to the growth of e-transactions in West Africa due to challenges on the validity of electronic messages and e-signatures

145 The Guardian "ECOWAS moves to harmonise cyberlaws for e-commerce" 06 April 2015 available at https://guardian.ng/ecowas (date of use: 26 June 2020).

146 UNCTAD "Summary of adoption of e-commerce legislation worldwide" In the ECOWAS region, countries with e-transaction laws are: Benin, Burkina Faso, Cabo-Verde, Cote d'Ivore, Gambia, Ghana, Guinea, Liberia, Senegal, and Togo. Sierra Leone has no legislation while Guinea Bissau, Niger and Nigeria have draft laws, available at www.unctad.org (date of use: 03 July 2020).

147 For the purpose of harmonisation of e-transaction laws in the ECOWAS region a supplementary Act on e-transactions was adopted, UNCTAD *Review of e-commerce legislation* 5.

148 Supplementary Act A/SA.2/01/10 on Electronic Transactions in the ECOWAS Area adopted at the 37th Session of the Authority of Heads of State and Government Abuja, 16 February 2010.

149 See article 9(2)(a) of ECOWAS Supplementary Protocol A/SP.1/06/06 amending the revised treaty of 1 June 2006.

by the provision of e-commerce specific law embodying personal data, the use of intellectual property online; and the taxation of e-commerce.[150]

5.5.1.1 Provisions

The ECOWAS E-transactions Act applies to commercial communications in whatever form,[151] and allows the transmission of e-contract information to any party.[152] Although not expressly indicated, the Act would appear to apply to both B2C and B2B transactions as certain of its provisions indicate situations specific to B2B transaction, while the general sections are consumer focused.[153] Nonetheless, there is no definition of who constitutes a consumer in terms of the Act. Reference may however, be made to the definition of a consumer in another ECOWAS regional document[154] which defines a consumer as "a natural person who uses or requests a publicly accessible telecommunication service for non-business purposes." The law, therefore, is aimed primarily at the protection of natural persons and therefore excludes juristic persons or entities from the protection afforded to natural persons.

Chapter 2 of the ECOWAS E-transactions Act is devoted to e-commerce. It provides for easy, direct, and sustained access to a supplier's information.[155] The required information includes: name of the supplier; geographic address; supplier's registration and tax information; prices including taxes and delivery cost; as well as information pertaining to professional codes, where applicable.[156] The provisions of the ECOWAS E-transaction Act make suppliers liable for the performance of all obligations in a

150 Preamble to the ECOWAS E-transactions Act.
151 ECOWAS E-transactions Act art 2; Orji (2018) 29/6 *ICCLR 375.*
152 ECOWAS E-transactions Act arts 16-18.
153 See ECOWAS E-transactions Act art 21.
154 ECOWAS Supplementary Act A/SA 1/01/07 on the Harmonisation of Policies and of the Regula tory Framework for the Information and Communications Technology (ICT) Sector, 2007.
155 ECOWAS E-transactions Act art 5.
156 ECOWAS E-transactions Act art 4.

consumer contract. Suppliers are however, relieved of liability where failure is evidently attributable to the other party, or to a situation beyond the control of the supplier.[157] Electronic advertising and spam are addressed in Chapter 3 of the ECOWAS E-transactions Act. Advertisements and offers must be clearly indicated without misleading headings or information,[158] while direct prospecting or communication which constitutes spam is prohibited outright. The medium of communication is irrelevant, provided the message is electronically sent without the consent of the recipient. When direct communication is sent in terms of the ECOWAS E-transactions Act, it must include a cost-free, opt-out procedure.[159] The control of spam under this Act is based on the opt-in approach, by which unsolicited communication is prohibited *ab initio*. Spammers are therefore placed on the defensive and bear the onus of showing that there was prior consent before the commercial communication was sent to the recipient.[160]

Chapter 4 of the ECOWAS E-transactions Act builds on Chapter 2 by providing further conditions for the validation of an e-contract. It provides that where there are conditions and provisions relating to the fulfilment of a contract, these terms and conditions must be available in a format that makes them possible to be recorded and reproduced.[161] The provisions should include steps to be followed in the execution of the contract electronically. Technical means of identifying and correcting errors; language of use; retention of and access to records; and professional rules to which the supplier is subject, where applicable should be explicitly provided.[162] For an e-contract to be validly concluded within the region, the consumer must be given the option to review the details of his or her order before confirmation.[163] It is important to note, that communication by either party is only complete once the party to whom the communication is addressed provides an acknowledgement. The provisions of the

157 ECOWAS E-transactions Act art 6 compared with art 5(2) of the AU Convention, the wordings of both Acts are the same so promoting harmonisation.
158 ECOWAS E-transactions Act art 8.
159 ECOWAS E-transactions Act art 13.
160 See similar provisions under art 4 of the AU Convention.
161 ECOWAS E-transactions Act art 19.
162 Ibid.
163 ECOWAS E-transactions Act art 20.

ECOWAS E-transactions Act consistently follow the information theory. This theory is encapsulated in article 28 and provides that "submission of a document in electronic form shall be considered effective when the addressee, after having read it, acknowledges receipt of the document."[164]

As with virtually all other provisions, article 7 of the ECOWAS E-transactions Act corresponds to the AU Convention in terms of applicable law, and also reflects international standards on the issue.[165] It provides that in the absence of a choice of law by the contracting parties, the applicable law shall be the law of the member state within the ECOWAS region "on whose territory the person carrying out the activity is established."[166]

In the ECOWAS E-transactions Act, writing and signature in electronic form are acceptable except in respect of private agreements as indicated under the exceptions.[167] According to article 32 of the Act, all transactions covered in the Act shall be admitted in evidence as proof in like manner as a hard copy with same evidential weight upon identification of the person from whom it emanates and the integrity of the process of getting the document. This provision reflects the intent of the UNCITRAL Model Law in giving recognition and evidential weight to e-documents.[168] Parties can also by agreement stipulate the terms of their contract.[169]

5.5.1.2 Exclusions

The ECOWAS E-transactions Act does not apply to "legally-authorised gambling, even in the form of bets and lotteries; legal representation and assistance services; and activities carried out by notaries public in application of the law."[170] Where writing is

164 Orji (2018) 29/6 *ICCLR* 381.
165 See again, art 3(1) of E-commerce Directive.
166 See art 3 of the AU Convention.
167 ECOWAS E-transaction Act art 3.
168 ECOWAS E-transactions Act arts 34-35; see further Orji (2018) *International Company and Commercial Law Review* 8.
169 ECOWAS E-transaction Act art 35.
170 ECOWAS E-transactions Act art 3.

required, the electronic equivalence of writing is not permitted for private acts relating to the law of the family and succession; and private acts "relating to personal or real, civil or commercial securities, except where these are entered into by an individual for the requirements of his (or her) profession."[171]

5.5.1.3 Limitations

Although the ECOWAS E-transactions Act had been incorporated by eight of its member states with legislative process ongoing in five other member states as of 2015,[172] the ECOWAS E-transactions Act is somewhat out of date in light of the rapid development of technology. New forms of e-transaction, such as mobile commerce and online auction platforms, are not addressed and there is no provision for steps which payment systems must follow in order to secure consumer transactions, and there are no safeguards against unfair trade terms. The Act fails to provide effective mechanisms for dispute resolution outside of mundane court practices. Remedies available to consumers in the exercise of their rights are also grossly inadequate.

5.5.1.4 Summary

The ECOWAS E-transactions Act replicates the provisions of the AU Convention thus creating a contextual balance and uniformity in e-transaction legislation within the ECOWAS region and to an extent, within Africa as a continent. The one different aspect relates to electronic invoicing where stringent safeguards are to be implemented under article 6(5) of the AU Convention before an invoice can be authenticated. However, the requirement for an invoice under article 31 of the ECOWAS E-transactions Act deviates from that of the AU Convention and reflects the spirit of e-communication as an electronic invoice is accepted as the equivalent of a hard copy, provided the integrity of the content can be guaranteed. The amendment and implementation of the

171 ECOWAS E-transactions Act art 26.

172 UNCTAD *Review of e-commerce legislation* 6, besides the Review by UNCTAD in 2015 there has been no known official update of the incorporation of the ECOWAS E-transactions Act by other member states.

ECOWAS E-transactions Act within the region will without doubt improve the protection available to e-commerce consumers in Africa, especially the West African region.

5.6 Organisation for the Harmonisation of Business Law in Africa

The Organisation for the Harmonisation of Business Law in Africa (OHADA) is an international organisation with membership drawn largely from the African Francophone states,[173] although membership is open to all African states and to countries outside of Africa which have been invited by state parties.[174] The movement for the harmonisation of business law in Africa law began in 1963 and took its foundation in 1991. And in 1993 the treaty establishing OHADA was signed by fourteen states.[175] Two states[176] later joined the OHADA and another state joined in 2012.[177] The OHADA treaty was revised in 2008 with the establishment of various institutions including: "the Conference of Heads of State and Government; the Council of Ministers; the Permanent Secretariat; the Common Court of Justice and Arbitration (the CCJA); and the Regional Training Center for Legal Officers (ERSUMA)."[178] The OHADA's primary aim is to create a harmonised system in the African region while still respecting national traditions in law and history. This way there would be no imposition of new legal or court systems.[179]

For the time being, the OHADA has no e-commerce-specific legislation, the Uniform Act Relating to General Commercial Law (Uniform Act), however, establishes the recognition and use of e-communication and e-signature, and also provides for the

---

173 Membership of OHADA is currently made up of seventeen countries: Benin, Burkina Faso, Cameroon, Central African Republic, Chad, the Federal Islamic Republic of the Comoros, Congo, Cote d'Ivoire, Equatorial Guinea, Gabon, Guinea, Guinea-Bissau, Mali, Niger, RDC, Senegal, and Togo, see OHADA "General overview" available at www.ohada.org (date of use: 09 September 2020).

174 Treaty on the Harmonisation of Business Law in Africa (OHADA Treaty) revised 2008 art 53.

175 OHADA "History of OHADA" available at https://www.ohada.org (date of use: 15 March 2020).

176 See Mouloul *Harmonisation* 18, the states of Comoros and Guinea later joined.

177 The Democratic Republic of Congo completed its adhesion in 2012 bringing the number of member states to seventeen, see Houanye & Shen (2013) 4 *Beijing Law Review* 1.

178 Mouloul *Harmonisation* 30.

179 Martor, Sellers & Pilkington *Business Law in Africa* 19.

online filing of applications.[180] To that extent, the relevant provisions of the Uniform Commercial Law will be given due consideration in this study.

5.6.1 Uniform Act Relating to General Commercial Law 2014

The Uniform Act Relating to General Commercial Law (Uniform Act) 2014 (revised), repeals the Uniform Act of 17 April 1997 on General Commercial Law. The Uniform Act is a bulky piece of legislation and has 307 articles arranged in nine books with titles covering diverse areas. These books are further sub-divided into chapters addressing the following titles: the status of merchant and enterpreneur;[181] register of commerce and securities;[182] national registry;[183] computerisation of the register of commerce and securities;[184] national and regional registries;[185] lease for professional use and enterprises;[186] commercial intermediaries;[187] commercial sale;[188] and finally, transactional and final provisions.[189] Book Five which deals with the computerisation of the register of national and regional registries touches on the recognition of electronic records and will therefore form the basis of the study of e-communication under OHADA law.

5.6.1.1 Provisions

The Uniform Act applies to any merchant, be it a natural or legal entity, or entrepreneur, including all commercial companies and public institutions.[190] The Uniform Act also applies to any economic interest group located in any state that is a signatory to the Treaty on the Harmonisation of Business Law in Africa. The Uniform Act further

180 UNCTAD *Review of e-commerce legislation* 5.
181 This is contained in Book 1 of the Uniform Act from arts 2-33.
182 Uniform Act Book 2 arts 34-72.
183 Uniform Act Book 3 arts 73-75.
184 Uniform Act Book 4 arts 76-78.
185 Uniform Act Book 5 arts 79-100.
186 Uniform Act Book 6 arts 101-168.
187 Uniform Act Book 7 arts 169-233.
188 Uniform Act Book 8 arts 234-302.
189 Uniform Act Book 9 arts 303-307.
190 Uniform Act art 1.

provides that all those subject to it – ie, merchants and entrepreneurs – remain subject to the laws of the state where the business is registered or established provided those laws are not contrary to the Uniform Act.[191] Book Five of the Uniform Act provides an opportunity for the authorisation of the application of e-documents and e-signatures in the OHADA states, even in consumer transactions.[192] The Uniform Act further provides for the computerisation of the register of commerce and securities and lists general principles for use of electronic procedures, which can be applied by national and regional registries.[193] It also provides rules for validating e-documents and e-signatures.[194] There is provision for the use and conservation of e-documents;[195] the use of electronic means for the transmission of documents;[196] as well as publicity and electronic dissemination of register of information.[197]

As a protective measure for parties – and consumers in particular – the Uniform Act authorises the use of both hard and electronic copies in its registries for all formalities or applications, provided they can be sent and received by the recipients using the same form of communication. The standardisation of procedures performed through the use of documents and electronic procedures is vested in a Technical Committee established within the OHADA.[198] E-documents have the same legal effects as hard copies which means e-documents are valid and may be used as evidence.[199] However, for e-documents to be so recognised they must be stored by a reliable technique which can, at any time, guarantee the origin of the document and its integrity during electronic processing and transmission.

191 Ibid.
192 Uniform Act art 79.
193 Uniform Act arts 79-81.
194 Uniform Act arts 82-85.
195 Uniform Act arts 86-91.
196 Uniform Act arts 92-96.
197 Uniform Act arts 97-100.
198 Uniform Act art 81.
199 Uniform Act art 81.

The Act also authenticates the use of a qualified e-signature on the conditions that: it is associated with the user; it allows for proper identification of the user; it is created in a way that ensures that the signatory is the sole person to have exclusive control over the signature; and the signature is linked to a particular document in order to trace future alterations.[200] As regards a qualified signature, the Uniform Act provides that for an e-signature to be classified as qualified, it must consist of software for signature creation and verification, and must include an electronic certificate verifying the signatory, which must be produced by an approved provider. The criteria for the recognition of a provider are determined by the Technical Committee for the Standardisation of Electronic Procedures as provided under the Uniform Act.[201] The approach adopted in the Uniform Act to receipt and dispatch is interesting. There is an assumption that a piece of information is sent when it is received at the other end, and deemed to have been transmitted where compatibility between the information system of transmitters and receivers has been enabled. Where such information is received, it falls on the recipient to acknowledge receipt. The acknowledgement must bear the qualified electronic signature of the clerk or representative of the receiving body.[202] The Uniform Act further encourages e-data by providing for the certification of e-documents under article 98.

5.6.1.2 Limitations

As earlier noted, the Uniform Act is not specific to e-transactions and from the provisions considered above, it is clear that although the use of e-communication is valid and admissible in evidence, the provisions are not adequate for adaptation to consumer transactions. Rights of consumers must be specifically provided for in order to enable enforcement.

200 Uniform Act art 83.
201 Ibid.
202 Uniform Act art 96.

Following the above is an exploration of the level of protection available to e-commerce consumers within national borders in Africa. As was indicated earlier on in this chapter, e-transaction and online consumer protection laws are not in force in all countries in Africa.[203] The point of departure here is on studying the protection of an e-commerce consumer in a jurisdiction with e-commerce-specific legislation, such as South Africa, compared to a jurisdiction with no e-commerce specific legislation as will be seen in the Nigeria case in Chapter 8 of this study.

5.7 South Africa

5.7.1 Background

South Africa is a highly industrialised country in Africa with great potential for growth in technology and e-commerce.[204] Related to e-commerce development are issues on consumer protection and legal readiness. Fortunately, South Africa plays a leading role as regards law reform and legal development through the activities of the South African Law Reform Commission and the justice sector. As a member of the UN South Africa adopted the UNCITRAL Model Law in 2002 and enacted the ECTA which is largely influenced by the UNCITRAL Model Law.[205] It is noteworthy that RECs such as the SADC and COMESA have e-transaction instruments which are largely influenced by the ECTA and thus have similar provisions as will be seen in the foregoing paragraphs. In addition to legislation, case law is emerging in the area of cyber law. It is, therefore, extremely instructive to study the e-commerce consumer protection measures available in South-Africa as a mirror of current trends in consumer protection on the African continent from the perspective of national laws. Governance in South Africa is based on a three-tier system of government made up of the

203 See para 5.1.

204 Esselaar and Miller (2002) 2/1 *SAJIC 4,* Jobodwana ZN (2009) 4/4 *Journal of International Commercial Law and Technology* 288.

205 UNCITRAL "UNCITRAL Model Law on Electronic Commerce (1996) – Status" available at www.uncitral.org (Date of use: 28 October 2020); UNCITRAL "Status: United Nations Convention on the use of Electronic Communications in International Contracts (New York, 2005) available at www.uncitral.org (date of use: 28 October 2020).

executive, the legislature, and the judiciary. The judicial system is unified and has a national character, and is, therefore, not subject to provincial or local authorities. The provinces, however, have their own legislative houses but laws are made by the National Assembly after consideration by the National Council of Provinces (NCOP).[206]

5.7.2 Regulatory framework

Consumers in South Africa are generally protected under the Consumer Protection Act (CPA) which has extensive provisions on consumer protection. These provisions notwithstanding, consumers who transact online receive further protection through the provisions of the Electronic Communications and Transactions Act (ECTA)[207] which is the principal legislation governing e-transactions. Consumers are further protected in South Africa by a series of self-regulatory guidelines and codes. Among these codes are the Code of the Advertising Standards Authority (ASA) now administered by the Advertising Regulatory Board,[208] and the Code of Ethics and Standards of Practice of the Marketing Guidelines of the Direct Marketing Association of South Africa (DMASA).[209] These codes do not, however, fall within the scope of this chapter.

5.7.3 Electronic Communications and Transactions Act 2002

The ECTA seeks to remove and prevent barriers to the use of e-communications and transactions in the Republic; thereby promoting legal certainty and trust in the electronic market, amongst other objectives.[210] While consumers are specifically protected under the ECTA, section 3 makes it clear that the ECTA "must not be interpreted to exclude (the application of) any statutory or common-law provisions to

206 Government of South Africa "Structure and Functions of the South African Government" available at www.gov.za/about-government (date of use: 20 September 2020).

207 Act 25 of 2002 as amended by Consumer Protection Act 68 of 2008 (Notice 917 *GG* 33581 of 23 September 2010).

208 ARB "Welcome to the Advertising Regulatory Board" available at www.arb.org.za (date of use: 20 June 2020).

209 See more particularly para 12.5 of the Code of Ethics and Standards of Practice of DMASA available at https://www.outprosys.com/dma (date of use: 20 June 2020).

210 ECTA s 2.

electronic transactions." This extra protection from other legal instruments as envisaged in section 3 creates opportunities for consumer protection under the CPA. The CPA appears to have more detailed provisions in the areas of unsolicited goods and fair marketing and business practices as will be seen in paragraph 5.7.3.1 below. The ECTA aims to be technology neutral[211] and according to section 4, it is not required that persons must make use of e-communications in any transaction, neither does the ECTA prohibit any person from establishing requirements in respect of how he or she will accept data messages.

The ECTA applies to both commercial and non-commercial communications[212] and provides for the facilitation and regulation of e-communications and transactions. Most of the provisions of the ECTA implement the UNCITRAL Model Law on E-commerce.[213] South Africa is a partner to the OECD through its contribution to the OECD's work[214] and is thus expected to gain from the provisions of the OECD Recommendations and Guidelines on Consumer Protection. The ECTA covers virtually every aspect of electronic law including cyber-crimes and data protection so minimising the pitfalls inherent in fragmented legislation.

Chapter 7 of the ECTA specifically sets out measures to guarantee that consumers are not at a disadvantage when transacting electronically in comparison to when engaged in conventional transactions. These measures are, however, not an end in themselves as there are circumstances in which the Act will not avail the consumer. These limitations are spelt out in the paragraphs below dealing with consumer protection.

5.7.3.1 Provisions

Chapter 1 of the ECTA contains interpretation, objects, and application. Part 1 of Chapter 2 is a glimpse into the national electronic strategy, and Part 2 sets out the e-

211 ECTA s 2(f); see further Jacobs (2004) 16 *South African Mercantile Law Journal* 557.
212 ECTA at s 1.
213 See Stassen (2002) *De Rebus* 48.
214 OECD "South Africa and the OECD" available at www.oecd.org (date of use: 15 October 2020).

transactions policy. The next chapter, Chapter 3, addresses the legal requirements for data messages in Part 1, while Part 2 deals with the communication of data messages. Chapter 4 applies to e-government services and Chapter 5 to cryptography providers. Subsequent chapters address: authentication of service providers; consumer protection; protection of personal information; protection of critical databases; domain name authority and administration; limitation of liability of service providers; and cyber inspectors, cybercrime, and general provisions. This study deals specifically with the protection of e-commerce consumers which is detailed in Chapter 7 of the ECTA.

For present purposes, the scope of application of the ECTA; the principles underlying consumer protection in line with the rights of consumers; the limited liability of service providers; unfair terms in consumer contracts; expectations in payment systems; as well as jurisdiction and strategies for implementation, will be the focus of our study of the ECTA.

The core of consumer protection laws are the principles which they embody. It is the scope of these principles that measures the extent of protection afforded. One such principle is the recognition of e-communications. Chapter 7 of the ECTA provides a functional equivalence for e-communications in order to meet the requirements of: writing; signature; originality; retention; and reproduction. Section 15 of the ECTA specifically retains the integrity of e-communications and grants such documents or messages evidential value and this same recognition applies to automated transactions.

(a) Recognition of data messages and incorporated terms

The ECTA gives legal recognition and force to communications in data form.[215] Not only that, but terms or information which are not contained in an e-document or agree-

[215] See ECTA ss 3 and 11, these sections compare well with art 5 of the UNCITRAL Model Law and also reflect the same positions in the SADC Model Law ss 4 & 5 and the COMESA Model Law art 8.

ment but are referred to, also have legal force provided that the information is conspicuously referred to.[216] However, a term that is calculated to mislead or deceive will not enjoy the protection of the law. In *George v Fairmead (Pty) Ltd,*[217] a lodger signed on the register, a general indemnity. The Court however, nullified the signed document on the ground that the attention of the guest was not drawn to the relevant document before he appended his signature.[218]

It is further required that the information should be readily accessible in a form in which it can be read, stored, and retrieved.[219] The terms must be included in such a way that a reasonable buyer would take note of their inclusion or of reference to them. Under South African law, the supplier is also required to ensure that incorporated terms are brought to the attention of the buyer, failing which those terms will be excluded from the contract.[220] However, the fact that such terms were properly referred to, does not guarantee their enforceability as they must also be conscionable.[221]

In *Dlovo v Brian Porter Motors*,[222] the appellant (Dlovo) whose car was stolen in the respondent's premises before it was found, counter claimed to have the car repaired. Her claim was, however, contested based on the job card she had signed in which the respondent was exempted from liability arising from theft or loss. The court was quoted as follows:

> in the court *a quo*, the clauses were held to be enforceable, however, on appeal the court held that where a signatory is able to show that he or she was misled as to the nature of the

---

216 ECTA s 11(3); find a similar provision in art 9 of the COMESA Model Law. See further, Jacobs (2004) 16 *South African Mercantile Law Journal* 558.

217 *George v Fairmead (Pty) Ltd* 1958 (2) SA 465 (A) (hereafter the *Fairmead* case).

218 The *Fairmead* case 470B-E.

219 Section 11 of the ECTA implements art 5*bis* of the UNCITRAL Model Law and covers terms contained in shrink-, click- and web-wrap agreements. See for further reading on the disposition of the law towards linked or referred terms, Pistorius (2004) 16 *SA Merc LJ* 568; Pistorius (1993) 5 *SA Merc LJ* 1.

220 On these principles see *Africa Solar v Divwatt* 2002 (4) SA 681 (SCA); *King's Car Hire (Pty) Ltd v Wakeling* 1970 (4) SA 640 (N) 643-644.

221 Naude (2009) 126 *SALJ* 505; Naude (2006) 17 *Stell LR* 361.

222 *Dlovo v Brian Porter Motors* 1994 (2) SA 518 (C).

document, its purport, or its content, the doctrine of *caveat subscriptor* will not apply as the signatory would have acted under *justus error*.[223]

(b) Writing

A document in the form of a data message which is accessible for subsequent use fulfils the requirement of writing in any law in the Republic.[224] Data is generally categorised as indirect communication[225] as there is no direct interaction between the parties. Although data could be instantaneous, any difficulties in transmission or receipt of the message may not be immediately apparent.[226] Voice communications, such as telephone conversations or internet calls,[227] are regarded as direct forms of communication[228] and do not form part of data messages unless the voice is automated or stored in terms of section 1 of the ECTA.

(c) Signature

The physical appendage of a signature to documents is a deep-rooted legal requirement that could be problematic in the electronic age.[229] Online transactions notwithstanding, for most countries the requirement of a physical signature remains the norm,[230] especially in countries with no specific e-transaction legislation or a data-friendly law on evidence. This position has now been remedied in South Africa under the ECTA. The ECTA provides two standards applicable to the recognition of an e-signature. The first standard applies where the requirement of a signature is based on

223 Quoted from Koornhof (2012) 2 *Speculum Juris* 54.

224 See the case of *Sihlali v South African Broadcasting Corporation Ltd* (J700108) (2010) ZALC 1; (2010) 31 ILJ 1477 (L) where at issue was whether a resignation by SMS was valid resignation in terms of the requirement of writing (para 2). In para 18, the court held that a communication by SMS "is a communication in writing" (para 18) by relying on s 12 of the EC-TA.

225 See Christie and Bradfield *Law of Contract* 81-82.

226 Van der Merwe *Information and Communications Law* 160.

Internet calls are also known as voice over internet protocol (VOIP) by the use of applications such as what's-app or skype.

228 See *Tel Peda Investigation Bureau (Pty) Ltd v Van Zyl* 1965 (4) SA 475 (E); *Jamieson v Sabin-go* 2002 (4) SA 49 (SCA) para 5; *Odendaal v Nobert* 1973 (2) SA 749 (R).

229 UNCITRAL *Promoting Confidence in Electronic Commerce: Legal Issues on International Use of Electronic Authentication and Signature Methods* (2009).

230 Wright *Electronic Commerce* s 16.4-s 16.5; Baum and Perritt *Electronic Contracting* 337-341; Eiselen (1999) 6 *EDI LR* 21-46.

statutory provisions;[231] while the second applies where parties to a contract require an e-signature but fail to specify the type of e-signature to be used. For the first standard – where a signature is required by law without providing a specific format – the requirement is met, provided an advanced e-signature is used.[232] On the other hand, the second standard is met if a method is used to identify the signatory and to indicate his or her approval of the information communicated.[233] In the case of *Spring Forest Trading v Willberry (pty)*[234] the parties had a meeting to discuss the Appellant's default to the Respondent in respect of their rental agreement. The representative of the Appellant subsequently wrote an e-mail to the Respondent's representative outlining four proposals emanating from their meeting and in a subsequent e-mail; choose the option to cancel their rental agreement.[235] The Respondent disputed the validity of the e-mails stating that they were mere negotiations as there were no signatures appended on them.[236] The court held that the contract between the parties was a transaction in terms of the ECTA[237] and that the attitude of courts to e-signatures is pragmatic not formalistic. The court looks at whether the form of the signature on the document fulfils the function of a signature and not on how the signature looks.[238] The court further held that the names of the parties at the foot of the e-mails constituted data and sufficiently served as signatures.[239]

In all cases, where an advanced e-signature is used, there is a presumption that the e-signature is valid and has been properly applied until the contrary is proved.[240]

---

231 ECTA s 13.

232 ECTA s 13(1); it is important to note that, an advanced e-signature is defined in the Act as an electronic signature which results from a process which has been accredited by the Accreditation Authority see s 1.

233 ECTA s 13(3).

234 *Spring Forest Trading 599 cc v Willberry (Pty) Ltd t/a Ecowash and Another* 2014 (2) SA 118 (SCA).

235 *Spring Forest Trading 599 cc v Willberry (Pty) Ltd* (2) SA 118 (SCA) para 7.

236 *Spring Forest Trading 599 cc v Willberry (Pty) Ltd* (2) SA 118 (SCA) para 11.

237 *Spring Forest Trading 599 cc v Willberry (Pty) Ltd* (2) SA 118 (SCA) para 15.

238 *Spring Forest Trading 599 cc v Willberry (Pty) Ltd* (2) SA 118 (SCA) para 26.

239 *Spring Forest Trading 599 cc v Willberry (Pty) Ltd* (2) SA 118 (SCA) para 28; see also the case of *Macdonald & others v The Master & others* 2002 (3) SA 64 (N) on the use of data to satisfy the requirements of writing and signature.

240 ECTA s 13(4).

Communications or agreements in e-contracts have legal force with or without an e-signature. All that is required is that the document is evidenced by other means which show the maker's intention or statements, provided an e-signature was not expressly required.[241]

(d) Original

An e-document which is capable of being displayed or produced to the person to whom it is presented, and which has retained its integrity from the time it was first generated in its final form as a data message, satisfies the requirement of an original document.[242]

(e) Automated transactions

Transactions concluded by means of an AMS are given due recognition in the ECTA.[243] Section 20(c) of the ECTA validates contracts concluded with e-agents irrespective of any errors provided there is provision for a review of the contract terms before confirmation. Where however, there is no provision for review that transaction will be unenforceable.

(f) Electronic contracts

Contracts concluded by means of data messages are valid and enforceable.[244] The applicable sections of the ECTA dealing with the communication of data messages, act as default rules in the event that the parties involved in the communications have not reached an agreement on the applicable modalities of the contract. This provision implements article 4 of the UNCITRAL Model Law on variation by agreement. Parties are always at liberty to prescribe the mode of carrying out their transaction, including the manner in which acceptance can be expressed.[245]

---

241 ECTA s 13, compare with art 7 of the UNCITRAL Model Law; art 8 of the COMESA Model Law and s 7 of the SADC Model Law on the same principle.

242 ECTA s 14, this section is reflective of the provision of art 8 of the UNCITRAL Model Law.

243 Provisions enabling the use of AMS are similarly found in art 13 of the COMESA Model Law and s 16 of the SADC Model Law.

244 Jobodwana (2009) 4/4 *Journal of International Commercial Law and Technology* 292.

245 ECTA s 21; see also *Kergeulen Sealing and Whaling Co Ltd v CIR* 1939 AD 487.

The ECTA incorporates relevant provisions governing e-commerce and consumer protection as regards: the formation and validity of electronic agreements; the time and place of communications, dispatch and receipt; and the acknowledgement of receipt.[246] Under South African law, a contract involving direct communication is formed by relying on the information theory;[247] while where acceptance is by post, the expedition theory is applied.[248] In the case of e-contracts involving data communications or indirect communication, section 22 (2) of the ECTA provides that a contract is formed at the time when and place where the acceptance of the offer is received by the offeror. It is immaterial whether or not the recipient views or retrieves the message.[249] Section 23 of the ECTA is a restatement of the position in article 15 of the UNCITRAL Model Law which provides categorically that data used for the conclusion of a contract is deemed as received by the addressee the moment it is sent by the originator to the addressee. The section puts the place from where the data was sent as the registered place of business of the originator. And further provides that data is deemed received whenever it is capable of being retrieved by the addressee. The same rule on location of parties also applies to the addressee, thus providing that the data would be seen as received at the regular place of business of the addressee.

246 Article 11 of the UNCITRAL Model Law gives legal effect to the conclusion of e-contracts and agreements, while the rules on dispatch and receipt of e-communication as well the determination of the location of parties are provided in art 15 of the same law. Similarly, art 12 of the COMESA Model Law and s 10 of the SADC Model Law permits the use of e-communication for the formation and conclusion of online contracts while regulations on receipt and dispatch are contained in arts 14 and 19 of the COMESA Model Law and s 14 of the SADC Model Law.

247 Under the information theory, an offer is only effective when the offeree gets to know of it and acceptance is only effective when it is communicated to the offeror. The contract is only final and binding when the offeror obtains subjective knowledge of the acceptance. See further, Van der Merwe et al *Information Technology Law* 158; *Driftwood Properties (Pty) Ltd v McLean* 1971 (3) SA 591 (A) 597D-G; Cupido "Offer and acceptance in cross-border electronic contracts: A brief comparative perspective" 2015 3 available at www.ase-scoop.org (date of use: 05 September 2020).

248 For a comprehensive discussion on the conclusion of an internet contract see Pistorius and Hurter "Contracting on the Internet: The Formation of Contracts, Trade Practices and Online Dispute Resolution" 5; see also Schlechtrein *Commentary CISG* 163-165; Bagraim (1998) 2/6 *Juta's Business Law* 51.

249 This section of the law was tested in the case of *Jafta v Ezemvelo KZN Wildlife* (2008) 10 BLLR 954 (LC) where the court upheld a contract of employment between the parties notwithstanding the time the offeror only became aware of the acceptance made by the offeree. See Stoop (2009) 21 *SA Merc LJ* 110-125 for commentary on the case.

The dynamism of this rule on location is that it dispenses with the challenge of proving the place of establishment of a business or the location of its server in determining the location of parties.

Section 24 of the ECTA provides for the legal recognition of an expression of intent or other statement between an originator and the addressee in an e-communication while provision is further made for the attribution of data messages to the originator.[250] This position allows the recipient of an electronic message enjoy the protection of the law when dealing with an e-agent of the originator following the principle of consensus based on reliance.[251]

(g) Consumer protection

Chapter 7 of the ECTA, which addresses consumer protection, applies only to e-transactions between consumers and suppliers, but excludes financial services, auctions, and the supply of foodstuffs, beverages, or goods for everyday consumption.[252] It provides for a seven-day cooling off period to enable consumers perfect or withdraw their orders. The consumer-protection measure in exercise of the seven-day cooling off period as contained in Chapter 7 of the ECTA does not apply to services wich began with the consumers consent before the end of the seven-day cooling-off period, or to the supply of goods that are subject to fluctuations, or to the supply of goods made specifically to the consumer's specifications. Furthermore, the Chapter does not apply to goods that by their nature cannot be returned, or are subject to rapid deterioration or expiry. The protection in the Chapter does not also extend to transactions involving the purchase of unsealed audio or video recordings; the sale of newspapers, periodicals, magazines, and books; transactions for the provision of

250 ECTA s 25.

251 Van der Merwe et al *Contract: General Principles (2012)* 33-37; *Sonap Petroleum (SA) (Pty) Ltd v Papadogianis* 1992 (3) SA 234 (A) 2381-241D.

252 See s 44 ECTA; see also Jobodwana (2009) 4/4 *Journal of International Commercial Law and Technology* 294.

gaming and lottery services; and services for the provision of accommodation, transport, catering or leisure services.[253]

Most importantly, Chapter 7 of the ECTA does not apply to regulatory bodies established by law that deals specifically with consumer protection in respect of certain e-transactions. This presupposes that South Africans enjoy further protection for specific e-transactions such as financial services, privacy, and similar issues, without reference to the ECTA.[254]

In terms of the provisions of sections 43-48 of the ECTA the following consumer-protection measures are provided:

(a) information requirements regarding a business;[255]
(b) information requirements regarding goods;[256]
(c) the right to review and correct mistakes;[257]
(d) secure payment systems;[258]
(e) the right to cancel or withdraw from a transaction during a cooling-off period of seven or fourteen days (whichever period applies) without cost except the cost of returning the goods;[259]
(f) the principles governing unsolicited (goods),[260] services, or communications;[261]
(g) performance within 30 days of an order;[262]

253 The consumer protection measures contained in Chapter 7 of the ECTA are reproduced almost verbatim in arts 23-27 of the COMESA Model Law and ss 25-28 & 30 of the SADC Model Law. These provisions require a seven days cooling off period for cancellations and refund of any prior payment within 30 days of the cancellation. The consistency in the provisions of the various laws on e-transaction across the Southern region of Africa promotes certainty in e-commerce and builds trust in consumers.

254 ECTA s 42.

255 ECTA s 43(1) (a)-(g).

256 ECTA s 43(1) (h)-(n).

257 ECTA s 43(2).

258 ECTA s 43(5).

259 ECTA s 43(4); Jacobs (2004) 16 *South African Mercantile Law Journal* 561.

260 Although the subtitle of the ECTA in s 45 refers to unsolicited goods, the body of the law itself is silent on rules pertaining to unsolicited goods.

261 South Africa has made judicial progress in the fight against unsolicited commercial communications or spam, see *Ketler Investments CC t/a Ketler Presentations v Internet Service Providers' Association* (2014) 1 All SA 566 (GSJ) para 30. The ECTA also prescribes punishment against spam in s 45(4).

(i) protection by the inclusion of a standard clause under section 48 of the ECTA which nullifies any exclusion or web agreement that offends the rights of consumers as contained in the ECTA; and

(j) the right to a refund when orders are cancelled, or when there is no performance within 30 days of an order having been placed.[263]

When considering the benefit of a cooling-off period which includes the opportunity for a consumer to reconsider his or her choice in an e-transaction, attention must be drawn to the calculation of the cooling-off and withdrawal periods as provided in the ECTA. Firstly, consumers may cancel a transaction without reason *within seven days*. But the ECTA goes on to provide an additional period of seven days – so allowing a cooling-off period of *fourteen days* – but only in the following circumstances:

- where the supplier fails to meet the information requirements; or
- where the supplier fails to provide consumers with the opportunity to review their transaction.

The position, therefore, is that if the supplier is not in breach of the provisions of the ECTA, the cooling-off period is seven days. The calculation of both the seven and the fourteen-day periods is not cumulative but applies differently under different circumstances as explained above. The calculation of the fourteen-day period (where applicable) is *within* fourteen days of receiving the goods or services under the transaction.[264] In addition, where the transaction is cancelled for no reason, the calculation is within seven days *after* the date of receipt of the goods or of the conclusion of a service contract.[265]

The above provisions addressing the two distinct periods allowed for cancellation are not in conflict, as argued by some highly respected and learned writers. According to

262 ECTA s 46.
263 ECTA s 44(3).
264 ECTA s 43(3).
265 ECTA s 44(1).

Buys,[266] it is possible to estimate the total number of days for a cooling-off period to exceed 21 days. The writer calculates this based on his interpretation of section 44[267] – calculation of the period starts on the date of agreement, and in section 43(3),[268] calculation of the period only starts when the service is received (possibly long after the initial seven-day period). His calculation of the periods is cumulative, thus totalling the earlier assumption of over 21 days. However, reading sections 43 and 44 of the ECTA, a cooling off period under whatever circumstances in South Africa would not exceed fourteen days.

In summary, the above principles are relatively comprehensive and are capable of ensuring that South African e-commerce consumers enjoy protection in line with international best practices.

(h) Limited liability of service providers

Under the consumer protection regime, there are instances where consumers suffer loss from purchases made on websites either directly or through navigations.[269] The question of liability then arises and the likely culprit is the website which the consumer visited. The culpability or otherwise of a website owner or service provider who gave access in consumer contracts therefore is an issue of concern in consumer protection. [270] However, following international rules on promoting e-commerce objectives, there is a limitation on the liability of service providers under the ECTA.[271] The limitation applies where:

---

266 Buys and Cronje (eds) *Cyberlaw @ SA* 148.

267 Section 44 provides that a consumer may decide to cancel without reason within 7 days after the date of receipt of the goods or conclusion of an agreement for services.

268 It is provided that if a supplier fails to comply with the provisions of the ECTA, the consumer may cancel the transaction within 14 days of receiving the goods or services under the transaction.

269 In the case of *Fair Housing Council of San Fernando Valley v Roomates.com LLC* 521 F.3d 1157 (2008) a distinction was drawn between a website that acts as both a service provider and a content provider. The role of the provider determines its liability see opinion on 1163. A site that provides a link or navigation to another site is also not responsible for the content of the other site. For more discussion on the liability of service providers see Bayer (2008) 1 *Victoria University of Wellington Working Paper Series* 2,7.

270 This same opinion is shared in Visser (2003) 11/1 *Juta's Business Law* 40.

271 In the EU ISP's are protected against strict liabilities in terms of arts 12 and 13 of the E-

(i) The service provider is a member of an industry representative body whose members are subject to a code of conduct which must be adopted and implemented by the service provider.[272]

(ii) The service provider limits its functions to mere transmission, catching, and provision of information location tools.[273]

(iii) The service provider has an agent whose responsibilities include receiving notices of infringement. The agent's contact information must also be accessible on the website of the service provider.[274]

The above protection of service providers notwithstanding, a competent court may order a service provider to terminate or prevent any unlawful activity in terms of the ECTA. An insight from the ECTA is its decisive procedures for a take-down notification in the event of an infringement. The procedures eliminate the argument on how best take-down notifications can be carried out. The ECTA provides that the take-down notification must be in writing and addressed by the complainant to the service provider or its designated agent. The notification in terms of section 77 must include the following information:

- full name and address of the complainant;
- the written or e-signature of the complainant;
- identification of the right that has allegedly been infringed;
- identification of the material or activity that is claimed to form the subject of unlawful activity;
- the remedial action required to be taken by the service provider in respect of the complaint;
- telephonic and electronic contact details of the complainant, if any;
- a statement that the complainant is acting in good faith; and
- a statement by the complainant that the information in the take-down notification is to his or her knowledge true and correct.

commerce Directive; their liabilities are also limited under ss 31-34 of the SADC Model Law. However, there are no similar provisions under the COMESA Model Law.

272 See ss 71 and 72 of the ECTA.

273 ECTA s 76.

274 ECTA s 75(2).

Should it be found that a take-down notification is wrongful, the person who lodged the complaint will be liable for damages, provided it is shown that the complainant had knowingly and materially misrepresented the facts contained in the notification. In any event, where a service provider acts on a take-down notification, he will not be liable for a wrongful take-down.

Service providers in South Africa are, in general, not under an obligation to monitor data which they transmit, or to seek out any unlawful activities.[275] Such an obligation may, however, arise from agreements or regulations to which the service provider is subject, or to court orders, or to any right to limitation of liability based on the common law or the Constitution of the Republic.[276]

(i) Secured payment system

It has been noted in the preceding paragraph that the ECTA does not protect consumer interests in relation to financial or banking services; however, consumers are generally protected by statute and common law and other financial regulations against fraud and banking related irregularities. A secured payment system is rudimentary in e-commerce consumer transactions as most payments are generally processed by means of e-payment systems.[277] Funds transferred online are debited from the consumer's account through card details. Consumers also make payments through bank transfers as this appears safer[278] and serves as a middle-ground between traditional banking and credit-card payment. Although there is no specific legislation governing internet banking and electronic fund transfers in South Africa,[279] the relationship between a customer and a bank where internet services are deployed, is that of a debtor to a creditor, or a mandator to a mandatory, as the case may be. Where a banking platform is used to transfer funds online, once the transfer has been

275 ECTA s 73.
276 ECTA s 79.
277 Amro (2016) 20 *Vindobona Journal of International Commercial Law & Arbitration* 19.
278 See Kulundu-Bitonye (1998) *Lesotho LJ* 67-86; Malan & Pretorius (2006) 69 *THRHR* 594-612 and (2007) 70*THRHR* 1-22; Schulze (2004) 16 SA *Merc LJ* 51-66.
279 Schulze (2004) 16 *SA Merc LJ* 57-58.

concluded, mistakes cannot be corrected by the bank through fund reversals except by court order.[280] Parties may however, resolve the payment issues and subsequently re-instruct the bank.[281] It is important to note that it is the receipt of funds at the destination of the recipient, which concludes the payment instruction. This means that where there is a failure to pay, jurisdiction will be founded at the location where payment ought to have been made.[282]

While considering the challenges involved in resolving mistakes in cross-border fund transfers, it should be borne in mind that paying by credit card poses the additional risks of fraud, misappropriation,[283] and misuse of personal financial details. This payment security challenge has become an impediment in the promotion of e-commerce in South Africa especially among small businesses.[284] That is not to say that there are no remedies, as web-traders who have failed to provide adequate security on their trading sites could be liable, especially in respect of the following:

(i) payment into and from wrong accounts;
(ii) payment that exceeds the agreed amount;
(iii) subsequent unauthorised payments;
(iv) willful or negligent disclosure and or use of a consumer's payment information by the supplier or his or her agents; and
(v) unauthorised access to and use of the consumer's payment information by third parties resulting from inadequate security on the supplier's network.[285]

280 *Nissan South Africa (Pty) Ltd v Marnitz NO and others (Stand 186 Aeroport (Pty) Ltd Interven ing)* (2006) 4 All SA 120 (SCA), 2005 (1) SA 441 (SCA).
281 Schulze (2004) 16 *SA Merc LJ* 68.
282 See *Bush and Others v BJ Kruger Incorporated and Another* (2013) 2 All SA 148 (GSJ) para 67.
283 Schulze (2005) 17 *SA Merc LJ* 202-213; see also OECD Working Party on the Information Economy Report DSTI/ ICCP/IE (2004) 18/FINAL of 18 April 2006, 5 available at www.oecd.org/sti/economy (date of use: 05 March 2020).
284 Cloete (2003) "SME's in South Africa: Acceptance and Adoption of e-Commerce" 8 available at www.researchgate.net (date of use: 16 August 2020).
285 Buys and Cronje (eds) *Cyberlaw @SA* 150.

(j) jurisdiction

For every consumer dispute where the parties are in different locations, determining the applicable law is a first step to resolving the issues, especially if the matter is before a civil court or tribunal. The usual steps in determining jurisdiction would generally include a location of the place where a contract was concluded; location of parties; presence of defendant or property within jurisdiction; subject matter; amongst others. In the ECTA, contracts are concluded at the time and place offeror received the acceptance.[286] This puts the conclusion of a contract at the place of the offeror. The offeror can be the consumer or supplier (in the case of a counter offer), which makes this provision indefinite. The ECTA only clearly provides for jurisdiction in criminal matters in respect of offences committed in South Africa or by a defendant within jurisdiction.[287] There is no challenge in determining jurisdiction in e-transactions within South Africa, but there could be in cross-border transactions – but then, jurisdictional issues in trans-border trade have always been a challenge.[288]

Looking beyond the ECTA, courts will not enforce the judgment of a foreign court if the foreign court lacks international competence in terms of South African law. In South Africa law, international competence for monetary claims is based only on physical presence,[289] residence, or submission of the defendant to the foreign court.[290] However, judgments from designated countries may be enforced in the Republic by virtue of the Enforcement of Foreign Civil Judgments Act (EFCJ Act).[291] The EFCJ Act provides that where a certified copy of a judgment from a designated country is registered by a clerk of the court in the Republic, the judgment shall have the same effect as a civil judgment of the court at which the judgment has been registered, and shall be enforced accordingly.[292]

286 ECTA S 22(2).
287 ECTA s 90.
288 See Snail (2008) 2 *JILT* 8.
289 *Richman v Ben-Tovim* 2007 (2) SA 283 (SCA).
290 Forsyth *Private International Law* 442-444; see also Lloyd (2013)13/7 *Without Prejudice* 80 available at www.withoutprejudice.co.za (date of use: 12 November 2020).
291 Act 32 of 1988.
292 EFCJ s 4.

Whatever the choice of law, South African consumers are protected in terms of Chapter 7 of the ECTA, irrespective of the applicable legal system.[293]

5.7.3.2 Exclusions

The ECTA does not apply to communications in wills,[294] the alienation of land, bills of exchange, or stamp duties.[295]

5.7.3.3 Limitations

The information requirements in the ECTA are not sufficiently comprehensive to protect m-consumers. There should be mandatory information provision for the use of mobile devices, bearing in mind their limited screen and storage capacity. In the era of digital products, there is the urgency to address suppliers' obligation to provide information on the operability of software for the operating device on which it will be installed.

The principle addressing unsolicited goods, services, or communications is inconclusive. The ECTA has failed to provide any rules in respect of unsolicited goods. It does not address the issue of liability and demand for payment from the consumer where unsolicited goods are delivered to him or her through online platforms. Is the consumer liable for associated damages; or will the consumer be forced to pay for goods or services which were not ordered? This fundamental lacuna in the ECTA requires urgent attention. E-commerce consumers can however fall back on the provisions of section 21 of the CPA which prohibits the sale of unsolicited goods and also rely on other protective sections which prohibit unfair marketing practices such as

293 ECTA s 47.

294 The exclusion of Wills from the scope of the ECTA may need to be revisited as a clear intention of a testator in the form of a data message has been recognized by the courts see the case of *Macdonald & others v The Master & others* 2002 (3) SA 64 (N); see also Snail and Matanzima (2011) *Without Prejudice* 61.

295 ECTA s 4(3); see further Schedule 1 of the ECTA for exceptions.

bait marketing; negative option marketing;[296] pyramid and multi-level marketing schemes.[297]

In line with the standard provision on commercial communications, especially in reference to the Consumer Protection Recommendations of the OECD,[298] the requirements that commercial communications should be easily identified, and that the identity of the sponsor of such communications must be disclosed, are conspicuously absent from the ECTA. E-commerce consumers may, however, fall back on the protection provided in s 69(4) of the Protection of Personal Information Act[299] which requires that direct commercial communications must include full details of the originator.

Furthermore, in order to avoid gaps which could lead to inadequate legislation, it is submitted that the provision for refunds should include a quantum by which to measure cost for damaged or partly-used goods. The ECTA should also include possible options available to both suppliers and consumers where, at the instance of the consumer, the cost of supplying the goods exceeds the regular cost, for example, the consumer chooses express delivery.

5.7.3.4 Enforcement and implementation in South Africa

By virtue of section 49 of the ECTA complaints should be directed to the Consumer Affairs Committee (CAFCOM). CAFCOM was established under section 2 of the Consumer Affairs (Unfair Business Practices) Act.[300] This latter Act has been repealed by the CPA and the functions of CAFCOM are now overseen by the National Consumer Commission (NCC) which is established under section 85 of the CPA. The

296 CPA ss 30-31.
297 CPA s 43; for a detailed discussion of consumer protection measures in the CPA see Jacobs, Stoop and Niekerk (2010) 13/3 *PER* 349.
298 Consumer Protection Regulations reg 14.
299 Protection of Personal Information Act 4 of 2013.
300 Act No 71 of 1988 now repealed by the CPA.

NCC is empowered to resolve consumer disputes arising from the CPA and any other law.[301]

Prior to the NCC, CAFCOM had investigative powers and managed the Consumer Investigations Directorate which proactively identified cases while reported cases were also resolved.[302] Disputes were resolved through ADR using the help of the Consumer Investigation Unit.[303] With the deployment of a consumer helpline, cases were reported in a variety of ways including telephonic, walk-ins, written, and referrals. In 2007/2008 CAFCOM reported a total of 1485 cases with a one-day turnaround time.[304] Presently, the NCC regulates consumer transactions in South Africa.[305] Consumers may make direct complaints to consumer courts, or tribunals within Provinces and complaints may also be made to regular courts. Class actions and complaints by consumer groups are nonetheless, permitted.[306]

5.8 Summary and conclusion

The possibilities and level of legal protection open to consumers in the course of their transactions online through the AU Convention and other regional instruments were considered in this chapter. The OHADA Uniform Law and a country specific law, the ECTA were also considered. Concern, however, arises when there is a comparative analysis of the provisions of these instruments and the fact that though they are provided within the African continent, they do not provide the same measures of protection. For instance, it must be borne in mind that states party to the OHADA treaty, are also subject to other regional laws which provide specifically for the use of electronic media in commercial transactions. Some OHADA state parties are also members of the SADC which has its own Model Law on E-transactions.

301 CPA s 85.
302 DTI *Consumer Affairs Committee Annual Report 2008/2009* available at https://www.gov.za (date of use: 19 October 2020) 20.
303 DTI *Consumer Affairs Committee Annual Report 2008/2009* available at https://www.gov.za (date of use: 19 October 2020) 27.
304 Ibid.
305 NCC "Welcome" available at www.thencc.gov.za (date of use: 15 October 2020).
306 CPA ss 69-78.

States party to the OHADA, are first and foremost, members of the AU and are expected to ratify the AU Convention on Cyber-security. Clearly, where there are two documents on a single topic – and especially where they contain conflicting provisions – one must take precedence over the other. In the case of OHADA states there is no need to look too far in that OHADA treaties are based on supranational powers, which implies supremacy over all other treaties from a different source but which cover the same fields. In terms of article 10 of the OHADA Treaty, once an "Act enters into force it becomes directly applicable and binding notwithstanding any contrary provision of the domestic law, be it anterior or posterior."[307] National constitutions, however, enjoy precedence over OHADA treaties.[308] If OHADA member states are committed to protecting their citizens from unfair business practices, the drive for harmonisation of business law must go beyond the OHADA and also be founded on a comprehensive framework of consumer protection principles.

The challenges posed by a proliferation of treaties on the same subject matter, is not an exclusive area of concern for OHADA state parties, in fact it is a general problem facing the African continent as a whole.[309] A comparative table is given below to highlight some of the areas of concern in the pursuit of consumer protection and the responses of different regions through their laws. These laws are placed alongside the UNCITRAL Model Law as a benchmark for international standards.

Table 5.2 Comparative table of evaluated laws in the African region

S/N	Is-sues	Support documents (from selected countries and regions)						
		UN-CIT-RAL ML 1999	AU Conv 2014	SADC ML 2012	ECO-WAS Act 2010	COME SA ML 2011	EAC Phas e 1 2008	OHA DA Uni Act 2014

307 For further reading see Mouloul *Harmonisation* 27.
308 Mouloul *Harmonisation* 28.
309 Lakhani (2015) *Vindbona Journal of International Law & Arbitration* 85.

1	**Validity of E-data**	Applicable article 5	Applicable article 6	Applicable ss 3-6	Applicable article 25	Applicable article 6	Applicable rule 5	Applicable articles 5 and 82
2	**E-sign**	Applicable article 7	Subject to certification article 7(3)	Applicable article 7	Applicable article 37	Applicable article 8	Applicable rules 5 and 13	Applicable article 83
3	**E-invoice**	Nil	Subject to authentication Article 6(5)	Nil	Applicable article 31		Nil	Nil
4	**E-notarisation/ce rtificate**	Nil	Nil	Applicable s.23	Nil	Applicable article 20	Applicable rules 13 and 14	Applicable article 98
5	**Adm & evidential weight of e-data**	Applicable article 9	Applicable article 6 (6)	Ss 19-20	Applicable articles 32, 33 and 36	Applicable article 10	Applicable rules 7	Applicable article 82
6	**Scope**	All commercial transactions article 1	All commercial transactions article 2	Any electronic transactions 3	All commercial transactions article 2	All commercial transactions article 1	All civil & Admin law matters rule 2	All merchants on territory of Member States
S/N	**ISSUES**	**UNCITRAL ML 1999**	**AU CONV 2914**	**SADC ML 2012**	**ECOWAS ACT 2010**	**COMESA ML 2011**	**EAC PHASE 1 2008**	**OHADA Uni Act 2014**
7	**E-Con-**	Article 11	Article 5 (1)	S 10	Article 17	Article 12	Applicable rule 6	Nil

	tract							
8	**Con-tracts by E-agents**	Appli-cable article 11		Applicable s 16	Nil	Applica-ble arti-cle 13	Appli-cable rule 6	Nil
9	**Ex-clu-sions**	By Member States article 1	Gam-bling, legal rep, acts of notaries article 2(1); Private deeds on family law & suc-cession, personal or com-mercial securities article 6(3)	Deeds on immovable property, wills, bills of exchange s 6(4); lease above 20 yrs s 7(5)	Gam-bling, legal rep, acts of notaries, Private agree-ments on family law & succes-sion, personal or com-mercial securi-ties	By Member States article 1	By Member States rule 6	Nil
10	**Ap-plica-ble Law**	Nil	Consum-er's loca-tion Arti-cle 3	Any law Ss 28 & 29	Place of estab-lish-ment/con sumer's location article 7	Nil	Nil	Nil
11	**Prese rva-tion of Right s/Unf air Term s**	Nil	Nil	s.29	Nil	Article 28	Nil	Nil
S/N	**Is-sues**	**UN-CITRAL ML**	**AU Conv 2014**	**SADC ML 2012**	**ECO-WAS Act 2010**	**COME-SA ML 2011**	**EAC Act Phase**	**OHA-DA Uni Act**

		1999					1 2008	2014
12	**Data Protection**	Another legislation; Guidelines for Personal Data Files 1990	Applicable chap 2	Another legislation; SADC Model Law on Data Protection 2011	Another legislation Supplementary Act on Personal Data 2010	Nil	Applicable rule 19	Nil
13	**Payment Security**	Nil	State laws article 7	Limited protections 25(1)	Nil	Limited protection article 23 (5)	Applicable rule 18	Nil
14	**Party Autonomy**	Applicable article 4	Applicable articles 3, 5(1) and 6(1)	Applicable s.3(2)(4) and s.11	Applicable article 23	Applicable art 4	Applicable r 3	Nil
15	**Incorporation by Reference**	Applicable article 5 *bis*	Nil	Applicable s.9	Nil	Nil	Applicable rule 6	Nil
16	**Information Requirements**	Another legislation; article 7 UN Convention on e-contracts	Applicable article 2(2)	Applicable s. 25	Applicable articles 4, 5 and 19	Applicable article 23	Applicable rule 18	Nil
17	**Time of Dispatch**	When in a system out of control of originator	Subject to acknowledgment by addressee article 6(4)	When in a system out of control of originator s.12	Acknowledgment articles 21 and 28	When in a system out of control of originator article 19 (1)	When in a system out of control of originator rule	When received by recipient article 96

		article 15					9	
18	**Time of Receipt**	When information enters designated sys or being capable of retrieval article 15	Nil	When information enters designated sys or being capable of retrieval s.13	Nil	When information enters designated sys or being capable of retrieval article 19 (2)	When information enters designated sys or being capable of retrieval rule 9	When received by recipient article 96
19	**Place of Dispatch**	Place of business or residence article 15	Nil	Place of business or residence s.14	Nil	Place of business or residence article 19(4)	Place of business or residence rule 9	Nil
20	**Place of Receipt**	Place of business or residence at 15	Nil	Place of business or residence s.14	Nil	Place of business or residence article 19(4)	Place of business or residence rule 9	Nil
21	**Direct Prospecting**	Nil	Prohibited-(opt-in) article 4(3)	Permissible (flexible opt in) s30	Prohibited(opt-in) article 4	Permissible (opt-out) article 25	Nil	Nil
S/N	**Issues**	**UNCITRAL ML 1999**	**AU Conv 2014**	**SADC ML 2012**	**ECOWAS Act 2010**	**COMESA ML 2011**	**EAC Phase 1 2008**	**OHADA Uni Act 2014**
22	**Unsolicited goods**	Nil	Nil	Nil	Nil	Implied art 25	Nil	Nil
23	**Right to Review**	Nil	Applicable article 5 (3)	Applicable s 25(2)	Applicable article 20	Applicable article 23 (2)	Nil	Nil

24	**Right to Cancel**	Nil	Nil	Within 14 days (Not exercisable for Not exercisable for Financial services, auction, consumables, goods with fluctuating price, unsealed software,gaming & lottery activities, sale of newspapers & periodical, accomodation, transport & catering services) s25(2)	Nil	Within 14 days (Not exercisable for Financial services, auction, consumables, goods with fluctuating price, unsealed software,gaming & lottery activities, sale of newspapers & periodical, accomodation, transport & catering services) article 22	Applicable rule 18	Nil
25	**Right to Performance**	Nil	Article 5 (6)	Within 30 days s.26	Article 6	Within 30 days article 26	Applicable rule 18	Nil
26	**Liability of ISP**	Nil	Nil	Limited ss 31-34	Obligation to perform article 6	Nil	Limited rule 11	Nil
27	**Take-down Notice**	Nil	Nil	Notice in form s.35	Nil	Nil	Implied rule 11	Nil

28	**Enforcement**	Nil	ADR article 33	Nil	Nil	Consumer complaints org/ODR articles 29 and 30	National agency rule 12	Nil
29	**E-transferable record**	Another leg. *UNCTRAL ML on E-transferable records 2017*	Nil	Nil	Nil	Nil	Nil	Nil
30	**E-auctions**	Nil	Nil	Nil	Nil	Nil	Nil	Nil
31	**Single windows**	Impliedly limited	Nil	Nil	Nil	Nil	Nil	Nil

The table above shows conflicting standards in the resolution of some of the issues raised. It also lays bare the functionality of the different laws in terms of coverage. It shows further that continental and regional protection of e-commerce consumers in Africa is provided in legislation so making it possible to do business online. However, this possibility is shrouded in a multiplicity of treaties. According to Borgen,[310] "the very success of treaties as a policy tool has caused a new dilemma: a surfeit of treaties that often overlap and, with increasing frequency, conflict (with each other.)" This situation has led to uncertainty and has rendered international law increasingly dysfunctional due to the sheer number of treaties.[311] A conflict between treaties is said to exist "where a party to two treaties cannot simultaneously honour its obligations under both,

310 Borgen (2005) "Resolving treaty conflicts" (2005) *Faculty Publications 122* 574 available at https://scholarship.law.st*john.edu/faculty_publications/122* (date of use: 05 October 2020).

311 Ibid.

whereas a divergence between both need not always be a conflict."[312] The resolution of conflicts in treaties can be found in article 30 of the Vienna Convention on the Law of Treaties, 1980. This article provides that where "all the parties to an earlier treaty (which is still in force) are also parties to a later treaty, the earlier treaty applies only to the extent that its provisions are compatible with those of the later treaty."[313] Various authors have pronounced on the issue, for example, Da Cruz Rodrigues proposes that the conflict should be equated with conflicts between domestic norms, and be resolved by applying basic concepts on superiority,[314] being that international laws are superior to regional laws.[315]

The above approaches notwithstanding, what stands out is the supremacy of an international treaty over a regional treaty. Moreover, in interpreting article 30 of the Vienna Convention it is apparent that the provisions of a later treaty or law will take precedence over an earlier one where both treaties are of a common origin.

Finally, the comparative table of evaluated laws in the African region shows some level of disparity and inadequacy in e-transaction legislation among the regional laws that were studied. Notwithstanding the existence of these regional laws some countries in Africa are yet to enact e-transaction legislation in their countries. For the purpose of protecting e-commerce consumers, African countries are encouraged to enact proper e-transaction legislation and to further ensure that their legislation reflects international standards. Meanwhile, regional communities in Africa will be better placed to protect the interests of e-commerce consumers on the adoption of a harmonised framework on e-transactions and consumer protection laws.[316] Presently, there are fourteen signatories and only five ratifications to the AU Convention.[317] Going by the provisions of

312 Jenks (1953) 30 *BYIL* 426.

313 The Vienna Convention on the Law of Treaties was opened for signature on 23 May 1969 and entered into force on 27 January 1980.

314 Mouloul *Harmonisation* 29.

315 Ibid.

316 Kiplagat (1995) 23/2 *Denver Journal of International Law and Policy* 284.

317 Benin, Chad, Comoros, Congo, Ghana, Guinea-Bissau, Mozambique, Mauritania, Rwanda, Si erra Leone, Sao Tome & Principe, Togo, Tunisia and Zambia are signatories while Ghana, Guinea, Mauritius, Namibia and Senegal have ratified the Convention see AU "African Union

article 36 of the AU Convention, the AU Convention is currently not in force.[318] The article provide as follows:

> This Convention shall enter into force thirty (30) days after the date of the receipt by the Chairperson of the Commission of the African Union of the fifteenth (15th) instrument of ratification.

Further on, a study of the South African legislation specific to e-commerce consumer protection was also undertaken in this chapter. It is observed that though e-commerce consumers are already entitled to the protection available under conventional consumer-protection laws in the Republic – for instance, the protection offered by the CPA – the electronic environment has peculiar challenges which differ from the regular purchase and sale in conventional space, and as such certain rules are required specifically to address these peculiar challenges. For instance, the CPA provides for the functions of the NNC for dispute resolution, but these functions are more in terms of the provisions of the CPA. On the other hand, cyber courts, ODR, and other online platforms are modern-day realities which are more suited for e-commerce more so, with capacity to deal with emerging technological issues.

In addition to the observation that the provisions of the COMESA Model Law and the SADC Model Law are in consonance with the provisions of the ECTA, it is also observed that virtually all the provisions in the ECTA are in line with those of the CRD and the E-commerce Directive. To that extent, the South African provisions correspond to the provisions in the EU with the result that consumers in EU buying from South African suppliers can be sure of enjoying more-or-less the same level of protection available in the EU – subject, of course, to filling the gaps of certain of the limitations identified in the preceding paragraphs. International principles established in the UNCITRAL Model Law, the EC Convention, and the AU Convention, , especially in the areas of the validity of e-data and its admissibility in evidence, contract formation, and

---

Convention on Cyber Security and Personal Data Protection" available at https://au.int (date of use: 26 June 2020).

318 See Orji (2018) 12/2 *Marsaryk University Journal of Law and Technology* 110; Amazouz "African Union perspectives on cybersecurity and cybercrime" 13.

applicable formalities, use of e-agents, and some other areas with limited modifications, are well embedded in the ECTA. An overview of South Africa's e-transaction legislation lends credence to the fact that with e-commerce and consumer-protection-specific laws, Africans are guaranteed of an effective consumer protection regime on par with the developed countries of the world.

The above notwithstanding, considering that the countries in Africa are enjoined to ratify and domesticate the AU Convention, it is rather unfortunate that the political will of African leaders to endorse the domestication of the Convention is low.[319] Finally, in view of the findings in this chapter it important that the AU Convention is reviewed in light of current developments. An updated Convention should attract better regional and national participation.

Chapter 6 diverges from regional to a national study of what countries outside Europe and Africa are doing to protect e-commerce consumers within their jurisdictions. The example for this detour is the US basically because of her old history in electronic consumption and the roles of their courts in resolving inter-state issues.

[319] The Convention has only been ratified by five countries and they are Ghana, Guinea, Mauritius, Namibia and Senegal available at http://au.int/en/treaties (date of use: 08 October 2020).

CHAPTER SIX

LESSONS FROM THE UNITED STATES OF AMERICA

6.1 Introduction

The US is a country that has successfully faced the challenges posed by e-communications in commerce through proactive and effective legal responses. Laws on e-commerce are well founded in case law and legislation in the US especially in the areas of jurisdiction, e-contracts, and liability of online intermediaries. The US's system of government is based on the division of powers between the legislative, judicial, and executive arms of government.[1] The executive arm includes the cabinet, executive departments, independent agencies, boards, commissions, and committees who together administer and enforce the laws of the country. Each State has her own laws while federal laws also controls the different States only to the extent provided in the Constitution under concurrent legislative functions.[2]

Bearing in mind the universal nature of internet regulation, most internet-related legislation was enacted by the National Conference of Commissioners on Uniform State Law.[3] The Uniform Law Commission (ULC) which was established in 1892 provides for states; non-partisan, well-conceived, and well drafted legislation that brings clarity, uniformity and stability to critical areas of state statutory law.[4] It studies and reviews the law of the states to determine which areas of law should be uniform. However, as the ULC can only propose the laws and recommend them to states for

1 US Government "How the US government is organised" available at https://usa.gov (date of use: 15 July 2020).

2 Ibid.

3 The Uniform Computer Information Transactions Act, 2002, and the Uniform Electronic Transactions Act, 2009, are principal laws on electronic transactions and were enacted by the National Conference of Commissioners on Uniform State Law.

4 Study.com "What is the Uniform Law Commission?" available at https://study.com (date of use: 30 November 2020).

implementation, a uniform law is ineffective in states until the state legislatures have adopted it.[5]

6.1.1 Regulatory framework

As indicated in the preceding paragraph, the regulatory framework for consumer protection in the US is contained in both Federal and State legislation.[6] For purposes of this study, e-commerce consumer protection laws under Federal statutes will be discussed. This legislation includes: the Uniform Electronic Transactions Act,[7] (UETA); the Controlling the Assault of Non-Solicited Pornography and Marketing Act,[8] (CAN-SPAM Act); the Electronic Signatures in Global and National Conference Act,[9] (E-SIGN Act); and the Uniform Computer Information Transactions Act,[10] (UCITA). Reference will also be made to the Restore Online Shopper's Confidence Act,[11] (Online Shopper Protection Act).

These e-commerce consumer laws are administered primarily by the Federal Trade Commission Agency (FTC) whose work is performed by the consumer protection, competition, and economics Bureaus.[12]

5 ULC *FAQ – How does an act receive final UCL approval?* available at www.uniformlaws.org (date of use: 01 July 2020).
6 Legal Aid Society Northeasthern NY "The differences between Federal, State, and Local Laws" available at https://www.lawhelp.org (date of use: 30 October 2020).
7 Uniform Electronic Transactions Act, 1999.
8 Controlling the Assault of Non-Solicited Pornography and Marketing Act, 2003, 15 USC Ch 103 ss 7701-7713.
9 Electronic Signatures in Global and National Conference Act, 2000, 15 USC Ch 96 ss 7001-7006.
10 Uniform Computer Information Transactions Act, 2002.
11 Online Shopper Protection Act, 2010, 15 USC Ch 110 ss 8401-8405.
12 FTC "Enforcement" available at https://ftc.gov>enforcement (date of use: 15 July 2020).

6.2 Uniform Electronic Transactions Act 2009

For the purpose of achieving uniformity, certainty, and predictability for consumers in the US in the retention of paper records through electronic records, the National Conference of Commissioners on Uniform State Laws proposed the UETA in 2009.[13]

6.2.1 Provisions

The UETA applies to electronic records and e-signatures relating to a transaction.[14] Section 3(15) of the UETA limits the application of the Act to the conduct of business, commercial, or government affairs. Although not specifically mentioned, the UETA applies to both B2C and B2B business e-transactions. The UETA applies prospectively to any electronic record or signature created, generated, sent, communicated, received, or stored on or after 1 January 2002.[15]

The UETA does not require that transactions are written or signed by electronic means; parties may choose the format of their communication in respect of any transaction[16] provided that where the transaction is to be carried out electronically, the scope must be subject to applicable e-regulations.[17] In terms of the UETA e-transactions are valid and can be enforced.[18] By virtue of section 5 of the UETA, party autonomy is recognised which means that parties' agreement may be varied. The UETA is technologically neutral and does not specify a particular technology for e-

13 Gabriel (2000) 5/4 *Uniform Law Review* 651-65; Reed (2001) 36/3 *Tort & Insurance Law Journal* 736; Fry (2001) 37/2 *Idaho Law Review* 248.

14 Witte (2002) 35/2 *The John Marshall Law Review* 316.

15 See Reed (2001) 36/3 *Tort & Insurance Law Journal* 740.

16 Parties do not need to change their business practices in favour of the use of electronic means, they simply need to agree on the most convenient means of executing their contract. This position is further discussed in Gabriel (2000) 5/4 *Uniform Law Review* 653; see also Boss (2001) 37/2 *Idaho Law Review* 293. .

17 UETA s 5; the UETA is focused on electronic or automated transactions falling within the mean ing of "transactions" as defined in the Act, Reed (2001) 36/3 *Tort & Insurance Law Journal* 738.

18 UETA ss 6 & 7; see also Amro (2016) 20 *Vindobona Journal of International Commercial Law & Arbitration* 15.

signatures.[19] Wherever a law specifies the requirements for the format of a document that requirement is met if it is provided in an electronic form capable of retention by the recipient at the time of receipt.[20] Where, however, the sender inhibits the ability of a recipient to store or print the electronic record, that record will be unenforceable against the recipient.[21] A problem that might arise here would lie in leading evidence to show that an inhibiting technology prevented the recipient from retaining the record. Would the inability of a recipient to retain a record due to inoperability or virus infection amount to the sender inhibiting the document? In my opinion, the answer is in the negative, since searching through some websites, it is possible to find web pages that cannot be downloaded or copied due to inhibiting technologies as envisaged in the Act – nonetheless, that premise will not account for all situations. Where such a case occurs it should be decided on the surrounding circumstances.

The UETA is based largely on the provisions of the EC Convention and the UNCITRAL Model Law,[22] and similarly, makes provision for the recognition of automated transactions, and the effect of errors.[23] It provides further for the attribution of electronic records and transactions,[24] the admissibility of electronic records into evidence,[25] electronic notarisation and acknowledgment of a document, as well as the electronic retention of records either in a plain form or in an original form which could be used for evidentiary, audit, or similar purposes.[26]

The UETA establishes a novel area by providing that where the retention of a cheque is required, that requirement is satisfied by retaining an electronic record of the information of both the front and back of the cheque provided that the information is

19 UETA s 7(d); see also Fry (2001) 37/2 *Idaho Law Review* 258.
20 See s 8 UETA.
21 Ibid.
22 Gabriel (2000) 5/4 *Uniform Law Review* 653; Boss (2001) 37/2 *Idaho Law Review* 283.
23 Fry (2001) 37/2 *Idaho Law Review* 263.
24 Gabriel (2000) 5/4 *Uniform Law Review* 655.
25 Fry (2001) 37/2 *Idaho Law Review* 264.
26 See arts 12 and 14 EC Convention and arts 8-10, 13-14 of the UNCITRAL Model Law on E-commerce, and compare with s 3(9-14) of UETA; for a discussion on the retention of electronic records under the UETA see Boss (2001) 37/2 *Idaho Law Review* 313.

accurate and accessible for future use.[27] In line with article 10 of the EC Convention, section 15 of the UETA provides procedural rules on time and place of dispatch and receipt of an electronic record. Under the UETA an electronic record is sent when it is properly addressed to a designated information processing system in which the recipient is able to retrieve the electronic record.[28] The electronic record is deemed to have been received when it enters the designated information system in a form that is capable of being processed by that system – it is immaterial whether or not the recipient is aware of its arrival in the system.[29] The place where an electronic record is sent or received is the party's place of business, especially the place having the closest link to the underlying transaction. And if the parties do not have a place of business, it will be their place of residence.

From our earlier study of different legislation on e-commerce and consumer protection both at international and regional levels, a persistent concern was that most of the provisions in these pieces of legislation were out-dated and could not address the gaps arising from newer technologies.[30] Part of that concern is taken care of here by the provision of an electronic version of a transferable record. The UETA entrenches the same rights and defences on a holder of a transferable record equivalent to a record or writing under the Uniform Commercial Code.[31] It further provides for the acceptance and distribution of electronic records by government agencies.[32]

27 UETA s 12(e).
28 Fry (2001) 37/2 *Idaho Law Review* 266.
29 UETA s 15(e).
30 See Comparative table of evaluated laws in the African region Chapter 5 para 5.8.
31 UETA s 16. The use of transferable record in the US can be traced back some twenty years when Federal Regulation provided for the use of electronic warehouse receipts in the cotton industry. Since then, certain negotiable electronic transferable instruments and negotiable electronic transferable documents have been recognised under US law see, for instance, the UETA s 16 and the Electronic Signatures in Global and National Commerce Act 15 USC 7001-7031 s 201. Furthermore, the holder of a transferable record under the UCC is expressed to have the same rights as a holder of an equivalent record in writing, such as an electronic transferable record, see Reed (2001) 36/3 *Tort & Insurance Law Journal* 743.
32 UETA s 17; Fry (2001) 37/2 *Idaho Law Review* 272.

The UETA has been adopted by 47 states in the US, and the District of Columbia, Puerto Rico, and the US Virgin Islands.[33]

6.2.1.1 Exclusions

The UETA does not apply to non-commercial transactions,[34] wills,[35] codicils, or testamentary trusts.[36] It also does not apply to transactions governed by the Uniform Commercial Code,[37] except for section 1.107 which has been repealed by amendment.[38]

6.3 Electronic Signatures in Global and National Commerce Act 2000

The enactment of the Electronic Signatures in Global and National Commerce Act (E-SIGN Act) in 2000 came in the wake of the UETA. This was necessary in order to minimize variations in e-signature law in states which had legislated on e-signatures based on the UETA.[39] The E-SIGN Act was signed into law almost immediately after the UETA and provides similarly for the recognition of electronic writing and signature.[40] It is a harmonised law regulating interstate and foreign commerce in the US.[41]

---

33 Thompson Reuters "Uniform Electronic Transactions Act (UETA)" available at https://content.next.westlaw.com (date of use: 19 June 2020).

34 UETA s 2(16).

35 The ULC at its meeting of 17 July 2019 passed a law to enable the recognition and execution of electronic wills and this law appears to be a first. The Uniform Electronic Will Act 2019 allows the execution of an electronic will. The will can be created, transmitted, signed and recorded electronically. The probate must give effect to an electronic will where the e-signature of the testator was witnessed contemporaneously. The electronic will must also be stored in a tamper-proof evident file, available at www.uniformlaw.org (date of use: 19 July 2020).

36 Fry (2001) 37/2 *Idaho Law Review* 252.

37 Uniform Commercial Code Act 174 of 1962 amended in 2012 and effective from 1 July 2013; see further Reed (2001) 36/3 *Tort & Insurance Law Journal* 742 and Dively (2000) 38/2 *Duquesne Law Review* 215.

38 UETA s 3(2); see also a further exemption in s 1.206 of the Uniform Commercial Code which has been amended to reflect that there shall not be a right of action for the sale of a personal property (not general goods) exceeding US$ 5 000 in amount or value unless the transaction was documented in writing.

39 Stern (2001) 16 *Berkeley Technology Law Journal* 399.

40 Reed (2001) 36/3 *Tort & Insurance Law Journal* 749.

41 E-SIGN Act ss 102 and 301; see Watson (2001) 53/4 *Baylor Law Review* 813.

6.3.1 Provisions

The E-SIGN validates data messages[42] and the use of digital signatures as an effective alternative to traditional ink-and-paper records and signatures.[43] It applies to consumer transactions and requires that consumers should be informed clearly of their right or option to access electronic records.

In the E-SIGN Act there are general rules on information which must be made available to consumers before they give consent. The information includes alternatives to electronic versions[44] and how to withdraw consent from electronic processing.[45] The E-SIGN Act further protects the consumer by requiring that before consenting to the application of electronic records, the consumer should have access to information on the hardware and software requirements necessary for retaining his or her electronic records.[46] Where there is a change in the hardware or software requirements which will pose a material risk such as limiting access, the consumer should be informed of these revised hardware and software requirements. In addition, following the change, the consumer should have the right to withdraw consent and to provide consent anew.[47] In essence consumers have a right to give or withdraw consent in respect of any electronic records without the imposition of a condition, consequence, or fee for a withdrawal.[48]

Electronic records which are required to be retained are to be retained by businesses and must accurately reflect the substance of the original record in an unalterable

---

42 E-SIGN s 101(e); see Zemnick (2001) 76/3 *Chicago-Kent Law Review* 1981; Hynick (2005) 12/1 *Southwestern Journal of Law and Trade in the Americas* 162.

43 E-SIGN Act s 101(a).

44 E-SIGN Act s101(c)(1)(B)(i); Stern (2001) 16 *Berkeley Technology Law Journal* 400.

45 E-SIGN Act s101(c)(1)(B)(iii).

46 E-SIGN Act s 101(c)(1)(C)(i); Stern (2001) 16 *Berkeley Technology Law Journal* 400; Hynick (2005) 12/1 *Southwestern Journal of Law and Trade in the Americas* 163.

47 E-SIGN Act s 101(c)(1)(D).

48 E-SIGN Act s 101(c).

format.[49] The records must be accessible and capable of reproduction for the legally required period.[50] The E-SIGN Act validates actions by e-agents provided that the actions are authorised by the person to be bound.[51] It prohibits discrimination in favour of or against the use of "a specific technology, process, or technique in creating, storing, generating, receiving, communicating, or authenticating electronic records or e-signatures",[52] thus standardising technological neutrality.[53] Under the E-SIGN Act, the most important safeguard is the ability of consumers to consent electronically or confirm consent electronically.[54] Therefore, a consumer whose consent is not obtained electronically is protected from the electronic processing of his or her personal information. Whereas the E-SIGN Act creates access to e-documents it, however, limits the misuse of e-documents thus preventing fraud and deception. Consumers are at liberty to directly seek remedies against unauthorised or fraudulent processing of their electronic records. Finally, the technological neutrality of the E-SIGN Act further ensures that e-transactions are readily available for the benefit of consumers.

6.3.1.1 Exclusions

E-signatures as provided in the Act are not recognised in the execution of wills,[55] divorce, and general matters of family law.[56] So also they do not apply to court documents, orders or notices.[57] Sections of the Uniform Commercial Code other than ss 1-107, 1-206 and articles 2 and 2A are basically excluded from the use of e-signatures.[58]

---

49 Adobe "US guide to electronic signatures. An overview of federal and state law" 2017 available at https://acrobat.adobe.com (date of use: 30 October 2020) 2.
50 E-SIGN Act s 101(d).
51 E-SIGN Act s 101(h); see further (2001) 36/3 *Tort & Insurance Law Journal* 749.
52 E-SIGN Act s 102(a)(2)(A); Stern (2001) 16 *Berkeley Technology Law Journal* 402.
53 Hynick (2005) 12/1 *Southwestern Journal of Law and Trade in the Americas* 163.
54 E-SIGN Act s 101 (c)(1)(c)(ii); see Zemnick (2001) 76/3 *Chicago-Kent Law Review* 1983.
55 This section of the E-SIGN Act will be modified and superseded by s 11 of the Uniform Electronic Wills Act 2019.
56 Hynick (2005) 12/1 *Southwestern Journal of Law and Trade in the Americas* 162
57 E-SIGN Act s 103.
58 Ibid; see also Watson (2001) 53/4 *Baylor Law Review* 816.

6.4 Controlling the Assault of Non-Solicited Pornography and Marketing Act 2003

The unpleasant experiences from receiving spam messages necessitated the enactment of the CAN-SPAM Act which was signed into law in December 2003.[59]

6.4.1 Provisions

The CAN-SPAM Act regulates commercial e-mails, establishes requirements for commercial messages, and gives recipients the right to stop e-mails from entering their mailboxes. It applies to any e-mail message the primary purpose of which is the commercial advertisement or promotion of a commercial product or service.[60] The CAN-SPAM Act requires that businesses obtain prior consent from recipients before engaging in sending them commercial messages.[61] Businesses may not use false or misleading header information in commercial communications and all commercial information must be easily identified and should include valid physical and postal addresses. The communication must include an opt-out request which must be handled promptly within no more than ten business days of an opt-out request.[62] The Act also provides for a Do-Not-E-Mail registry.[63]

Under the CAN-SPAM Act businesses are not relieved of their responsibilities – both the company whose product is promoted in the message and the company that actually sends the message may be held jointly liable where there is an infringement.[64]

---

59 Zhang (2005) *Berkeley Technology Law Journal* 318.

60 CAN SPAM Act s 5; see Zhang (2005) *Berkeley Technology Law Journal* 318; Kigerl (2009) 3/2 *International Journal of Cyber Criminology* 567.

61 CAN SPAM Act s 5(d)(2).

62 CAN SPAM Act s 5a (4)(A)(i).

63 CAN SPAM Act s 9a (1). The protection here is set out in the National Do-not-call Registry 15 USC Ch 87A s 6151; see Zhang (2005) *Berkeley Technology Law Journal* 322.

64 CAN SPAM Act s 6.

The CAN-SPAM Act provides penalties for violations, for instance, each e-mail in violation of the CAN-SPAM Act is subject to penalties of up to US$ 2 000 000.[65] The law further provides criminal penalties, including imprisonment for offences such as: accessing someone else's computer to send spam without permission; using false information to register for multiple e-mail accounts or domain names; relaying or re-transmitting multiple spam messages through a computer to mislead others as to the origin of the message;[66] harvesting e-mail addresses or generating them through a dictionary attack (the practice of sending e-mail to addresses made up of random letters and numbers in the hope of reaching valid addresses); and taking advantage of open relays or open proxies without permission.[67]

To minimize the effect of spam, ISPs include e-mail filters in their services and consumers can also register their lines on the FTC Do-Not-Call list in order to block off certain spam messages.[68]

6.5 Uniform Computer Information Transactions Act 2002

The Uniform Computer Information Transactions Act (UCITA) was the first uniform contract law designed to deal specifically with the new information economy.[69] It seeks to clarify and set out uniform legal principles applicable to computer information transactions in order to achieve predictability in the rules governing e-transactions.[70] The UCITA was drafted by the National Conference of Commissioners of Uniform State Laws in 2002. It has prefatory notes and comments and is divided into nine parts. Part I contains general provisions on scope, legal recognition of electronic

65 CAN SPAM Act s 7f (3)(b).
66 Army (2005) 33/4 *Pepperdine Law Review* 1042.
67 CAN SPAM Act s 7f (3)(b).
68 Zhang (2005) *Berkeley Technology Law Journal* 307.
69 Prefatory Note to UCITA. The provisions of the Act were under debate for almost a decade and most of its provisions have remained controversial. Critics of the Act believe that some provisions are not in the interest of consumers. More discussion on the criticism of the Act can be found in (2001) 36/3 *Tort & Insurance Law Journal* 746 & Shah *Berkeley Technology Law Journal* (2000) 15/1 91-93. Although the UNCITA does not appear to be of wide application in the US, see Wang (2015) 2 *Journal of Business Law* 95, a discussion of the Act is insightful in view of its details and wide coverage of issues on computer information transaction.
70 Shah *Berkeley Technology Law Journal* (2000) 15/1 104.

records, choice of law, unconscionable contracts, or terms; pre-transaction disclosures; and terms relating to interoperability and reverse engineering. Part 2 of the UCITA addresses issues in e-contract formation and terms of record, while Part 3 covers issues of construction as regards evidence and performance. Part 4 deals with warranties and Part 5 outlines rules on transfer of interests and rights. Part 6 of UCITA regulates performance; Part 7 sets out scenarios for breach of contract, cure for breach of contract, repudiation, and assurances. Part 8 of the UCITA provides for remedies and Part 9 contains miscellaneous provisions. The most relevant aspects of the law regarding e-commerce consumer protection are discussed below.

6.5.1 Provisions

The UCITA applies only to computer information transactions [71] and deals with contracts, not property law.[72] In a computer information transaction, the transferee seeks the information and contractual rights to use it.[73] Unlike a purchaser of goods, (eg, buyer, lessee, or licensee), a purchaser of computer information has little interest in the diskette or tape that originally contained the information once that information has been loaded onto a computer, unless the information remains on that media and nowhere else. And where the transaction is mixed – that is, it relates to both goods and computer information – the UCITA applies to that part of the transaction involving computer information, informational rights to it, and its creation or modification.[74] The UCITA also applies if the goods give the buyer or lessee access to or use of a

71 UCITA Prefatory Note.

72 Ibid.

73 The rights conveyed are informational rights that give access. It entails a limited or conditional transfer. Purchase of a copy gives certain rights to the use of that copy based on contract but does not convey intellectual property rights to the user, see Seo (2001) 1/146 *Buffalo Intellectual Property Law Journal* 146.

74 While the UCITA will apply to the computer information, the Uniform Commercial Code 1952 (UCC) will apply to the other part of the transaction if it forms part of its subject matter i.e. a computer; for more discussion see Seo (2001) 1/146 *Buffalo Intellectual Property Law Journal* 157*;* Shah *Berkeley Technology Law Journal* (2000) 15/1 89; see also Dively (2000) 38/2 *Duquesne Law Review* 227.

computer programme as a material purpose of transactions in goods of the type sold or leased.[75]

To drive home the scope of this Act, a consumer is defined as an "individual who is a licencee of information or informational rights that the individual at the time of contracting intended to be used primarily for personal, family, or household purposes."[76]

The rules in the UCITA are default rules which only apply when parties fail to specify some other rules. Principles are, however, set out for consumers of information records. These principles are discussed below.

6.5.1.1 Recognition of electronic records and automated message systems

In section 107, the UCITA gives legal recognition to electronic record authentication. It further recognises the use of e-agents or an AMS.[77] Parties are, however, permitted to set their own requirements.

6.5.1.2 Variation by agreement

Parties may vary the terms of their agreement save for the obligations of good faith, diligence, reasonableness, and care imposed by the UCITA. Terms which qualify as unconscionable and offend fundamental public policy, may not be included in a contract. Contract terms may also be limited in terms of agreed choice of law, choice of forum, requirements for manifesting assent, and the opportunity to review a transaction.[78]

---

75 UCITA s 103(b).
76 UCITA s 102.
77 Reed (2001) 36/3 *Tort & Insurance Law Journal* 747.
78 UCITA s 113(a); see further Shah *Berkeley Technology Law Journal* (2000) 15/1 90.

6.5.1.3 Information requirement and opportunity to review

A licensor which makes its computer information available to a licensee by electronic means from its internet or other devices must make the standard terms of the licence readily available for review by the licensee before the information is delivered, or before payment is made.[79] Consumers must be afforded an opportunity to review the contract terms before finally placing the order.[80] Consent to proceed with a transaction is required after review[81] and can be implied by an action such as a "click" or by other conduct.[82] The opportunity to review a record or term by a person or an e-agent exists only when it is made available in an accessible manner that is capable of reproduction. The requirement of access is satisfied if there is a conspicuous electronic link for the consumer's use. And where a supplier fails to provide an opportunity for the consumer to review the terms of the transaction before collecting charges, the consumer has a right of return and reimbursement if, after purchase, he or she sees the terms and does not agree to them. The right to return, however, falls away if the consumer had an opportunity to review the contract terms, but failed or neglected to use the opportunity.[83]

6.5.1.4 Time of receipt

The UCITA deals briefly with receipt of electronic information. It provides that an electronic message is effective when received even where the addressee is unaware of its receipt.[84] This provision appears too rigid and leaves no room for unforeseeable

79 UCITA s 112.
80 Wang (2015)2 *Journal of Business Law* 95.
81 UCITA s 112.
82 See *Register.Com, Inc v Verio, Inc* 126 F Supp 2d 238 (Dist Court SD New York 2000).
83 The opportunity to review is also designed to assist consumers to correct any errors. And where there is no opportunity to correct an error in an automated transaction, the transaction can be cancelled. Cancellation can however, only take place if the consumer, on learning of the error, promptly notifies the other party and causes delivery to the other party or his or her assignee of copies in his or her possession, or destroys them (if permitted to do so by the supplier), provided that the consumer has not used or received any benefit or value, directly or indirectly, from the information, see s 214 UCITA.
84 UCITA s 215(a).

circumstances. In terms of e-mail responses, a message may be delivered to an address, but the delivery may be to the recipients' junk folder. On the other hand, a recipient may receive a mail, delete it, and claim that the mail was never received. Further safeguards in this provision would be very useful in resolving the question of receipt and time of receipt in an information transaction. The UCITA also provides that receipt of an electronic acknowledgement establishes that the electronic message has been received. Nonetheless an acknowledgement is not a proof or confirmation of the content of a message or information.[85]

6.5.1.5 Prohibition of wrongful electronic self-help

Electronic self-help is using electronic means in exercise of a licensor's right. For example, a licensor could discontinue access if there is a material breach of access by cancelling a licence.[86] He or she can also take possession of all copies of the licenced information in the possession or control of the licensee, together with any other material relating to that information which by contract is to be returned or delivered by the licensee to the licensor.[87] However, wrongful self-help is prohibited in order not to breach the peace[88] and this occurs when the licensor acts outside the provision of the UCITA or without an order of court where required.

6.5.1.6 Warranty

The UCITA provides for both express and implied warranties.[89] Under the Act, advertisements can form part of an express warranty. Meanwhile, there is implied warranty of merchantability of computer programmes unless it is disclaimed or modified by the supplier (which is often the case). A licensor, who is a merchant with respect to computer programmes, warrants to its end user that the programme is fit for

85 UCITA s 214(b).
86 UCITA s 815; the debate on the provision of electronic self-help in the Act is discussed in Dively (2000) 38/2 *Duquesne Law Review* 249.
87 Ibid.
88 UCITA ss 815(b) and 816.
89 UCITA ss 403-409.

the ordinary purpose for which such computer programmes are used. There is also an implied warranty for informational content from a merchant who, in a special relationship of reliance with a licensee, collects, compiles, processes, provides, or transmits informational content. The implied warranty is that there is no inaccuracy in the information content,[90] but it would appear that there is no implied warranty for software which is provided free of charge.

6.5.1.7 Performance

Generally, performance must conform to contract.[91] Once performance is accepted, the party must pay or render the required consideration as agreed.[92] A party who accepts a performance has the burden of establishing a breach of contract with respect to the accepted performance. A performance may be refused if it does not conform to the contract.[93] A performance may also be cancelled if the breach is material and affects the entire contract. A cancellation under the UCITA is not effective until the canceling party gives notice to the party in breach.[94] An action for breach of contract must be commenced within four years after the right of action accrues, or one year after the breach has, or should have, been discovered, but not later than five years after the right of action accrues.[95]

90 UCITA s 404. By virtue of s 404 the implied warranty for information content does not include published informational content which should include on-line databases and contents of digital newsletters. It is argued that published informational content deserves as much protection as other information contents, on this discussion see Shah *Berkeley Technology Law Journal* (2000) 15/1 104 95.

91 UCITA s 601.

92 UCITA s 601(c)(3).

93 UCITA s 601(b)(1).

94 UCITA s 802(b).

95 UCITA s 805.

6.5.1.8 Remedies

The doctrine of *ubi jus ibi remedium*[96] is well enshrined in the UCITA. Breach of performance is, therefore, mitigated by remedies provided in the Act.[97] Parties may agree on remedies in their agreement in the unlikely event of a defect or breach. Remedies could be for replacement, repair, or refund. Some terms include a "no cancellation" policy but allows the exercise of other remedies; some businesses incorporate consequential-damage limits. But where any of these remedies fail, parties are obliged to approach the court for relief.[98] However, in terms of section 803 of the UCITA a disclaimer or limitation of consequential damage is enforceable.

Cases under personal injury against information providers have, even under tort law, been rejected by the courts. An illustrative case is *Sidney Blumenthal and Jacqueline & anor v Matt Drudge and America Online, Inc.*[99] In the *Blumenthal* case, Drudge had a website where he published the "Drudge Report," a gossip page with links to other on-line news. He had a wide viewership and was contracted by America Online (AOL) to post his material on the AOL website for one year at 3 000 US$ a month. In 1997 he wrote and transmitted a defamatory statement about the Blumenthals on his web page which he also sent to AOL. AOL, in turn, published the defamatory content and the matter was taken to court. AOL was joined in the suit against Drudge. Drudge immediately apologised and retracted his statements, while AOL applied for summary judgment relying on protection from the immunity sections in favour of ISPs in the Communications Decency Act.[100]

According to Wilkinson CJ:

---

96 This doctrine is founded on the latin maxim of where there is a wrong, there is a remedy. It is a protecttive doctrine on which an injured party can rely to claim legal right.

97 UCITA s 801; see also Reed (2001) 36/3 *Tort & Insurance Law Journal* 748.

98 Note that court in this Act is defined to include arbitral tribunals, regular courts, or other DR processes. Cyber courts are also envisaged.

99 *Sidney Blumenthal and Jacqueline & anor v Matt Drudge and America Online, Inc.*No CIV A 97-1968 PLF (1998) briefed from Electronic Frontier Education available at pdf https://www.eff.org (date of use: 06/11/2019)(hereafter the *Blumenthal* case)

100 The *Blumenthal* case 3.

> [Section] 230 of the Communications Decency Act creates Federal immunity to any cause of action that would make service providers liable for information originating with a third-party user of the service… thus, lawsuits seeking to hold a service provider liable for its exercise of a publisher's traditional editorial functions-such as deciding whether to publish, withdraw, postpone or alter content-are barred…congress has conferred immunity from tort liability as an incentive to service providers to self-police the internet for obscenity and other offensive material, even when the self-policing is unsuccessful or not even attempted.[101]

Therefore, AOL's application was granted based on immunity.

This shows that, in dealing with information products, the courts prefer to balance public interest in encouraging distribution of information, against interest in creating new sources of recovery.[102]

Damages could be measured with respect to performance that has been accepted and not properly revoked. This assessment could be based on the value of the performance required, less the value of the performance that has been rendered.[103] Damages could also be based on acceptance which was properly revoked; and the amount of any payment made and the value of other consideration given to the licensor with respect to that performance which had not been previously returned to the licencee. Other considerations include the market value of the performance less the contract fee; the cost of a commercially reasonable substitute transaction less the contract fee under the breached contract; or damages calculated in any reasonable manner.

Incidental and consequential damages can also be calculated provided that the damages measured do not exceed the market value of the performance that formed the subject of the breach. This form of damages includes restitution of any amount paid for performance not received and not accounted for within the indicated recovery. On the whole, the amount of damages must be subtracted from any unpaid contract fees for performance by the licensor which has been accepted by the licencee, and for

101 The *Blumenthal* case 6.
102 UCITA s 803.
103 UCITA s 804.

which the acceptance has not been properly revoked.[104] Furthermore, the law provides for recoupment. An aggrieved party may deduct from any payments due under the contract, all or any part of the damages resulting from the breach, after notifying the party in breach of the contract of its intention to make the deductions. Recoupment is permissible only if the agreement does not require further positive performance by the other party, and the amount of damage deducted can be readily liquidated under the agreement if the breach of contract is not material to the particular performance. Finally, specific performance may be ordered by a court.[105]

6.5.1.9 E-contracts

Part 2 of the UCITA sets out rules on contract formation; the general rule is that contracts above US$ 5 000 are unenforceable unless they have been placed on record and are in agreements not older than one year.[106] Failure to comply with this requirement does not render the contract void, but does preclude a party from relying on it as a defence, or bringing an action based on the contract. A contract may be formed in any manner which sufficiently evidences agreement.[107] An offer to conclude a contract may be accepted in any manner, including shipment or a promise to ship, or by commencing the contract with performance.[108] An offeror who is not notified of an acceptance or performance within a reasonable time, may treat the offer as having lapsed before performance. If an offer in an electronic message requires acceptance by an electronic reply, a contract is formed when the electronic acceptance is received.[109] If the acceptance is to be indicated by performance, it will be deemed to have been accepted once the performance has been received; while in the case of a request for access, performance is deemed once the access has been enabled.[110]

104 UCITA s 809.
105 UCITA s 811.
106 UCITA s 201.
107 Dively (2000) 38/2 *Duquesne Law Review* 233.
108 UCITA at s 203.
109 UCITA s 203(4).
110 UCITA s 203.

An acceptance can alter the terms of an offer if it contains material terms that vary the terms of the offer. In such an event, there will be no contract unless the party agrees by manifesting consent to the amended terms. Terms in an acceptance which conflict with terms in an offer are not part of the contract since conflicting terms in an acceptance are excluded by the UCITA. The Act defines a conflicting term as one that conflicts with the terms in an offer.[111] In like manner, it provides guidelines for contracts formed by or with e-agents in section 206.

An authenticated record that may not be altered or cancelled except by another authenticated record should not be altered or cancelled verbally or in any other way besides authentication.[112] Suffice it to say that a standard form supplied by a merchant to a consumer requiring an authenticated record before modification of a contract term, is not enforceable unless the consumer manifests assent to the modification.[113]

Generally, in an e-contract a party who assents to a record adopts that record and the terms of the contract, whether or not the record is in a standard form.[114] He or she is bound unless the term is unconscionable, constitutes fraud or similar conduct, or conflicts with a term to which the parties to the contract have expressly agreed.[115] In some contracts, the terms are only available after the initial stage of performance, although some contracts are layered and in some contracts dealing with software, the terms are generally “pay-now, terms-later.” The circumstances of each case determine the exercise of a right to return and to reimbursement. However, a licencee who agrees to a licence but receives a non-conforming product has a right to reject the copy and obtain a refund of the contract fee as a remedy for breach of contract.[116] Under this section, the right to return is cost free but does not include the use of an unreasonably expensive means of return, attorney fees, lost income, or the like.

111 UCITA s 204(d)(1).
112 UCITA s 303(b).
113 Ibid; Dively (2000) 38/2 *Duquesne Law Review* 235.
114 UCITA s 208; see Dively (2000) 38/2 *Duquesne Law Review* 233.
115 UCITA ss 208-209.
116 UCITA s 209 (b).

6.5.1.10 Unfair Terms

An unconscionable contract or term refers to terms that are one side and could cause oppression and unfair surprise on the consumer because of the superior bargaining power of the supplier.[117] The UCITA provides that if it is claimed or appears to the court that a contract or term is unconscionable, the parties must be afforded a reasonable opportunity to present evidence as to its commercial setting, purpose, and effect to assist the court in making a determination. And where the court finds, as a matter of law, that a contract or term was unconscionable at the time it was made, the court may refuse to enforce the contract, enforce the remainder of the contract without the unconscionable term, or limit the application of the unconscionable term so as to avoid an unconscionable result. This provision also applies to automated transactions where, because of a procedural breakdown in contract formation, there could be unexpected and oppressive results in the terms of the agreement.[118]

The UCITA provides that terms limiting interoperability and reverse engineering are unenforceable.[119] According to the UCITA

> a licensee that has lawfully obtained the right to use a copy of a computer programme, may identify, analyse, and use those elements of the programme necessary to achieve interoperability of an independently-created computer programme with other programs, including adapting or modifying the licensee's computer programme.[120]

Unfair terms in whatever form could work against the protection of a consumer by limiting usage, complaint mechanisms, jurisdiction, and on occasion, bind consumers

---

117 See commentary under s 111 of UCITA.

118 See *Intel Corp v Integraph* 195 F 3d 1346 (Fed Cir 1999); see also *Brower V Gateway 2000 Inc* 676 NYS 2d 569 (NYAD 1998).

119 Section 118 UCITA. This section also defines interoperability as the ability of computer pro grams to exchange information and of such programmes to mutually use the information that has been exchanged. While reverse engineering is a practice that involves close examination of a product that has been purchased in order to discern technological or other information that is discoverable from that product – where that technology is not protected by copyright, patent, or similar law, and the product is sold in the open market, under trade secret law. Reverse engineering is recognised as a proper means of acquiring information.

120 UCITA S 118.

to unknown future terms which may become applicable as the product is being used! To determine the validity of such exclusion clauses, the court looks at the circumstance of each case, together with substantive rules on the application of warranties. However, where such licences are conspicuous the court tends to enforce their terms unless they are unconscionable.[121] Unfair terms are prevalent in e-contracts through shrink wrap, click-wrap, or web-wrap agreements. These agreements contain exclusion clauses or warranties limiting liability and are disproportionate in that they cater in the main for the protection of the suppliers and increase their bargaining powers.[122] Shrink-wrap, click-wrap and web-wrap agreements are discussed below.

(a) Shrink-wrap agreement

Shrink-wrap licences are standard agreements, also known as contracts of adhesion,[123] and can dispense with the requirement of obtaining signatures to indicate assent.[124]

According to the US Court of Appeals, Seventh Circuit:

> The "shrink-wrap licence" got its name from the fact that retail software packages are covered in plastic or cellophane 'shrink-wrap', and certain vendors have written licences that become effective as soon as the customer tears the wrapping from the package.[125]

In *MA Mortenson Co v Timberline Software Corporation,*[126] the petitioner (MA Mortenson) purchased licenced software from the respondent and used it in the preparation of a construction bid. He however incurred losses and sued the respondent for breach of warranty for the defective software.[127] The respondent relied

---

121 Agreements are said to be "unconscionable where a clause or term in the contract is alleged to be one-sided or overly harsh...." see *Maynard Nelson v Mary McGoldrick* 127 Wn 2d 124 (1995) at 131.

122 Wilmerhale "The Origin of Click-Wrap: Software Shrink-Wrap Agreements" (2000) available at www.wilmerhale.com (date of use: 14 October 2020).

123 See further Burgess (1986) 15 *AA LR* 255.

124 Pistorius (2004) 16 *SA Merc LJ* 568.

125 See *ProCD Inc v Zeidenberg* 86 F 3d 1447 Court of Appeal 7th Circuit (1996); see also Seo (2001) 1/146 *Buffalo Intellectual Property Law Journal* 147.

126 *MA Mortenson Co v Timberline Software Corporation* 998 P 2d 305-Wash Supreme Court 2000 (hereafter *Mortenson* case).

127 *Mortenson* case 306.

on a term in the licence agreement which limited damages to recovery of the licence fee.[128] At the trial court, it was found, as a matter of law, that

> …the licensing agreements and limitations pertaining thereto were conspicuously displayed. Therefore, the remedies available to the plaintiff were those set out in the licensing agreement...[129]

This decision was upheld at the Court of Appeals having regard to the fact that the existence of a licence was noted on the screen each time the software was used.[130] The Washington Supreme Court found Mortenson's unconscionability claim unpersuasive and held the limitation of remedies clause to be enforceable.[131]

The court followed a similar line of reasoning in the case of *ProCD Inc v Zeidenberg,*[132] in this case, the Circuit Judges also held that "shrink-wrap licences are enforceable unless their terms are objectionable on grounds applicable to contracts…"[133] Here, ProCD had a compilation of telephone directories in a database "Select Phone (trademark) database".[134] He sold the database at different rates but based on personal or commercial use.[135] In order to manage the usage ProCD enclosed a licence in the software. The licence limited "use of the application programme and listings to non-commercial purposes."[136] Zeidenberg bought a consumer package and did not consider the licence. Instead he incorporated Silken Mountain Web Services Inc to resell the information in the "Select Phone (trademark) database."[137] Zeidenberg further bought two newer versions of ProCD's packages to update his database.[138]

---

128 *Mortenson* case 309.
129 *Mortenson* case 310.
130 *Mortenson* case 306.
131 *Mortenson* case 316.
132 *ProCD Inc* 86 F 3d 1447 (herafter the *ProCD* case).
133 The *ProCD* case 1449.
134 Ibid.
135 Ibid.
136 The *ProCD* case 1450.
137 Ibid.
138 Ibid.

ProCD sought "an injunction against further dissemination that exceeds the rights specified in the licences."[139] Although the District Court had held that shrink-wrap licences are not contracts, the Circuit Judges disagreed as in this case, the licence was in the software and the buyer had the opportunity to reject the purchase if the terms were unsatisfactory. Zeindergerg had this opportunity but decided not to use it.[140]

(b) Click-wrap

Click-wrap agreements are online agreements setting out the rights and obligations of the parties involved. The licences are sometimes displayed on the computer screen with a requirement to agree to the terms before proceeding.[141] The term "click-wrap" derives from the manner in which the agreement is entered into. To indicate acceptance, the user clicks on the "I agree" button or similar wording, before concluding the transaction. They are, in essence, self-executing, standardised online agreements – a "take it or leave it" form of contract with which the consumers can do little but comply.[142] Where the consumer clicks on the "I agree" or "I accept" button, or completes a registration or agreement form as an act of submitting to the terms of usage, the consumer becomes bound to the terms of the agreement. These agreements more often than not expressly exclude the usual implied warranties in merchantable products. However, in jurisdictions that prohibit the exclusion of implied warranties, such exclusions will not be enforced.[143]

Further on, click-wrap agreements are unilateral contracts requiring no particular format. In *Specht v Netscape Comms Corp*, [144] Hellertsein, the district judge, commented that:

---

139 Ibid.

140 The *ProCD* case 1452-1453.

141 Dively (2000) 38/2 *Duquesne Law Review* 240; see more on the discussion in Hull (2000) 51/6 *Hastings Law Journal* 1392.

142 Furmstom *Law of Contract* 21.

143 See s 31 of the UK Consumer Protection Act 2015 and s 56 of the CPA South Africa; see also Clarke "Why US Agreement Terms don't Always Work in Europe" pdf available at www.osbourneclarke.com (date of use: 14 October 2020).

144 *Specht v Netscape Comms Corp* 150 F Supp 2d 585- District Court SD New York (2001) (here after the *Specht* case).

> promises become binding when there is a meeting of the minds and consideration is exchanged.. assent may be registered by a signature, a handshake, or a click of a computer mouse transmitted across the invisible ether of the internet. Formality is not a requisite; any sign, symbol, or action, or even willful inaction, may create a contract, provided that it refers unequivocally to the promise…[145]

The peculiarity of this form of agreement is that they are one-sided agreements that basically tilt in favour of the supplier to the detriment of the consumer. Nonetheless, the consumer has no opportunity to modify or review the terms of the agreement as they are standardised. In view of this, most consumers do not bother to read the terms of such agreements before clicking on the agreement button. Agreeing to the terms without reading them deprives the consumer of protection. Consumers have two options: accept the terms; or walk away.

(c) Web-wrap

Web-wrap agreements – also known as browse-wrap agreements – are agreements entered into by a consumer through browsing web pages. The agreement is simply presented as terms and conditions, usually displayed by a hyperlink, which the user browses while visiting the site.[146] Very often, web-wrap agreements constitute an unacceptable form of agreement as no action which can reasonably amount to consent, is properly obtained in the course of merely browsing a webpage. According to Roberson,[147] consent cannot be obtained before reading the terms of an agreement. In most cases, the terms of use are not visibly displayed on the web page and there are also no restrictions on the user which subject him or her to the need to indicate consent before accessing the product or services in question. In web-wrap agreements, the argument of: "I was unaware of the existence of the alleged online terms", makes the courts cautious in upholding the validity of such agreements.[148] This is particularly so where in some cases the licence agreement does not form part of the web-page but appears on a different web page which is linked to the homepage.

145 The *Specht* case 587.
146 Pistorius (2004) 16 *SA Merc LJ* 570.
147 Robertson (2003) 78 *WLR* 275.
148 Pistorius (2004) 16 *SA Merc LJ* 572.

Although the fact that the licence agreement did not form part of the web page but was on a linked page is not sufficient reason for the courts to refuse to enforce the terms of the licence. Article 5*bis*[149] of the UNCITRAL Model Law provides that

> information shall not be denied legal effect, validity, or enforcement solely on the grounds that it is not contained in the data message purporting to give rise to such legal effect, but is merely referred to in that data message.

Such terms would be given effect to provided there are other factors – for example, the overt or implied act of the consumer which shows knowledge and acceptance of the incorporated reference or terms. This was the case in *Pollstar v Gigmania Ltd,*[150] where the plaintiff instituted three claims against Gigmania, one of which was for breach of contract based on a licence agreement.[151] The plaintiff alleged that it created and developed updated sensitive concert information which it published on a daily basis on its web site — www.pollstar.com—"at great time and cost".[152] The website was subject to a licence which the plaintiff claimed was a notice upon opening the website and that "by clicking on an access button to retrieve any of the information contained in the website, defendant agreed to be bound by the terms of the licence agreement."[153] The plaintiff alleged that the defendant over time had downloaded information from its website, which was used for commercial purposes against the terms of the licence.[154] The defendant argued that there was no expression of consent on the supposed licence and the action should fail accordingly.[155] The court viewed the website, and "agreed with the defendant that many visitors to the site may not be aware of the licence agreement. Notice of the licence agreement is provided by small gray text on a gray background."[156] The court further observed that although the

149 UNCITRAL Model Law 1996.
150 *Pollstar v Gigmania Ltd* 170 F Supp 2d 974 Dist Court ED California 2000 (hereafter the *Pollstar* case).
151 The *Pollstar* case 976.
152 The *Pollstar* case 977.
153 Ibid.
154 Ibid.
155 The *Pollstar* case 980.
156 The *Pollstar* case 980-981.

licence is on a linked page, but that since the notice leading to the linked page is in gray and is not highlighted; many users would not know that it was an active link.[157]

To avoid confusion and minimize litigation in consumer contracts, valid terms in a contract should be unequivocal and precise and not subject to the wishes of the contracting parties either to follow the terms or to ignore them. An unsigned document that contains contractual provisions cannot in itself constitute proof that the parties agreed to those terms.[158] While the law permits contracts to be concluded electronically in whatever format,[159] such contract terms and general conditions must be made available in a way that allows the consumer to store and reproduce them.[160] This requirement presupposes that such terms must be accessible and identifiable, and must be followed by an overt act by the consumer to indicate acceptance. In *Specht v Netscape Comm Corp*,[161] the court stated that in order for a contract to become binding, both parties must consent to be bound.[162]

The courts require that consent to the formation of a contract should be manifested in some way, by words or other conduct, if it is to be effective.[163] The onus, therefore, is on the party relying on the agreement to show that consent was reached. In the *Specht* case, the court had to determine whether by downloading free software on the defendant's site, the plaintiffs had agreed to the terms of the software licence which included an arbitration clause.[164] In downloading SmartDownload, the plaintiffs had also downloaded and installed communicator.[165] Communicator had a click wrap display of its licence but SmartDownload had none before downloading.[166] The click-wrap presentation for SmartDownload was only visible after downloading upon

157 The *Pollstar* case 981.
158 Van der Merwe et al *Contract: General Principles* 265-270.
159 See arts 9(1) and 11 of the E-commerce Directive.
160 E-commerce Directive art 10(3).
161 *Specht v Netscape Communications Corp* 306 F 3d 17 - Court of Appeals 2nd Circuit 2002 (hereafter *Specht* case).
162 *Specht* case 35.
163 See *Binder v Aetna Life Ins Co* Cal App 4th 832, 850 89 Cal Rptr 2d 540,552 (Cal Ct App 1999).
164 *Specht* case 18-20.
165 *Specht* case 23.
166 *Specht* case 24.

scrolling down.[167] The court concluded that plaintiffs had not assented to an arbitration clause under the SmartDownload licence terms as they could not have reasonably known of the licence which was hidden below the download button.[168] According to the court, a "reasonably conspicuous notice of the terms and unambiguous manifestation of assent to those terms by consumers are essential if electronic bargaining is to have integrity and credibility."[169]

It is submitted that consumers are adversely affected in the course of their online transactions, especially as they appear disinclined to read the terms of a licence before clicking to proceed. The consumers feel helpless when confronted with licences as a refusal would amount to denial, especially where alternatives with better licences are limited. Web owners appear to be aware of this and will exploit the position unless consumers challenge unfair terms.

6.5.1.11 Choice of Law

Parties in an e-contract may agree on a choice of law to govern their transaction.[170] Although a choice of forum clause is ordinarily valid and enforceable, such inputs may, however, be invalidated by law. Due to the nature of internet contracts which are usually contracts of adhesion, the validity of a choice of forum test will be respected provided it does not violate positive law, or is unconscionable.[171] In the US, unfair contract terms are covered in the UCITA which specifically provides that terms which are found to be unfair are generally unenforceable, and the courts will disregard those terms whether or not the agreement was signed by the consumer.

167 *Specht* case 23.
168 *Specht* case t 38.
169 *Specht* case 35.
170 Dively (2000) 38/2 *Duquesne Law Review* 231.
171 See the judgment of the court in *MA Mortenson CV Timber line software Corp* 998 P 2d 305 (Wash Supreme Court 2000) and *ProCD Inc v Zeindenberg* 86 F 3d 1447 (Court of Appeal 7th Circuit 1996) above where the court held that terms in the contracts were enforceable provided they did not offend public policy or were unconscionable.

The above notwithstanding, the UCITA enforces agreed choices of law by providing that parties may choose a law to apply to their transaction in the absence of an enforceable agreement on choice of law. In a global information economy, requirements that the selected choice of law must bear a reasonable relationship to the transaction are not necessary; parties may therefore choose a neutral location.[172] The only limitations are found in issues of unconscionability and the treatment of the overriding fundamental public policy of the forum state.[173] Parties may also choose an exclusive judicial or arbitral forum unless the choice is unreasonable or unjust.[174] Where, however, in the absence of an agreed choice of law the governing jurisdiction is outside of the US, that law will only govern if it provides substantially similar protection and rights as contained in the UCITA to the party not located in that jurisdiction.[175]

6.5.1.12 Exclusions

The UCITA does not apply to financial or insurance services or to agreements in relation to motion pictures or sound recording. It also does not apply to a compulsory licence, a contract of employment, or a contract that does not require that information be furnished as computer information.[176] Generally, the UCITA finds no application to the sale or lease of goods, or in contracts with insignificant computer information (on the basis of the *de minimis*-principle). It also does not apply to contracts for regulated telecommunication services and products; contracts for motion pictures, broadcasts, or cable programming.[177]

6.6 Restore Online Shopper's Confidence Act 2010

172 UCITA s 110.

173 See the cases of *Medtronic Inc v Janess* 729 F 2d 1395(11th Cir 1984); *Application Group Inc v Hunter Group Inc* 61 (App 4th 881, 72).

174 See the case of *Evolution Online Systems Inc v Koninklijke Nederland NV* 145 F 3d 505 (2nd Cir 1998).

175 UCITA s 109(c).

176 Ibid at s 103(d)(A)-(B) and s 103(d)(4-6); for the exceptions see generally Chanin (1999) 18 *John Marshall J Computer & Information Law* 293-294.

177 UCITA s 103(d).

Due to the ease with which consumers can be reached online, marketing has turned aggressive through the transfer of consumers' data by suppliers to third party sellers through a "data pass" process.[178] With "data pass" a supplier passes on a consumer's information (including bank or credit card details) to a "post-transaction third party seller" without the knowledge of the consumer. Section 8402(d)(2) of the Restore Online Shopper's Confidence Act defines a "post-transaction third party seller" as a person who:

(a) Sells, or offers for sale, any good or service on the internet;
(b) Solicits the purchase of such goods or services on the internet through an initial merchant after the consumer has initiated a transaction with the initial merchant;
(c) Is not -
    (i) the initial merchant;
    (ii) a subsidiary or corporate affiliate of the initial merchant; or
    (iii) a successor of an entity described in clause (i) or (ii).

Sometimes the consumer is registered in a free consumers' club and is contacted by a post-transaction third-party seller who the consumer mistakes for the initial supplier.[179] However, deception and fraud arise where consumers accept free trial versions of products thinking that they will be contacted for their payment information at the end of the period of the trial version. But with the "negative billing option" and an existing "data pass" arrangement, the post-transaction third- party sellers are able immediately to charge consumers without the consumers' input or consent.[180] The "negative billing option" approach enables a supplier to charge a consumer without his or her consent at the expiry of the period of a trial version. The consumer can only withdraw after his or her account has been debited, and then only against future deductions. These approaches of "data pass" and "negative billing option" are unfair to consumers. The objective of the Restore Online Shopper's Confidence Act is to prohibit these practices for the protection of consumers.

178 Restore Online Shopper's Confidence Act 2010 s 8401(4) (also known as the Online Shopper's Protection Act).
179 Restore Online Shopper's Confidence Act s 8401(1)(5).
180 Restore Online Shopper's Confidence Act s 8401(1)(8).

6.6.1 Provisions

The Restore Online Shopper's Confidence Act requires that before charging a consumer, a post-transaction third-party seller must make available all important terms of the contract. These must include the description of the goods or services, the cost, and a declaration that he or she is not affiliated to the initial merchant.[181] The post-transaction third party is prohibited from the use of the negative billing option and must receive express and informed consent from a consumer before giving effect to any charge. By this Act, an initial merchant is prohibited from disclosing a consumer's billing information to any post-transaction third-party seller through the use of a "data pass."[182]

6.7 Jurisdiction

Courts tend to accept the borderless nature of the internet and are very reluctant to consider the possibility that geographic distinctions could be drawn online. This is exemplified in the case of *America Library Association v Pataki*[183] where the US challenged a New York state law which sought to regulate obscene content online, whereas the court stated that the internet is wholly insensitive to geographic distinctions. In almost every case, users of the internet neither know nor care about the physical location of the internet they access.

Among the consumer protection laws of the US examined in this work, the UCITA specifically makes provision for jurisdiction under different trade agreements. It provides that in an access contract[184] or a contract providing for electronic delivery of a

181 Restore Online Shopper's Confidence Act s 8402(a).
182 Restore Online Shopper's Confidence Act s 8402(b).
183 *America Library Association v Pataki* 969 F Supp 160 (SDNY 1997).
184 An access contract is an agreement that authorises access to, or obtaining information from, an electronic facility. It includes contracts for remote data processing, remote access to applications software, or data stored on a third-party computer or third-party e-mail systems, and con-

copy, the law of the jurisdiction of the licensor will apply.[185] And in respect of consumer tangible copies, or a consumer contract which requires delivery of a copy in a tangible medium, the law of the jurisdiction in which the copy is or should have been delivered to the consumer applies.[186] In all other cases, the contract will be governed by the law of the jurisdiction having the most significant relationship to the transaction.[187] The location of a party is its headquarters, place of business, or the place of its incorporation or primary registration if it does not have a physical place of business, and in the case of an individual, the location is his or her address of primary residence.[188]

In the US, where parties are likely located in different States under different jurisdictions, exercising personal jurisdiction over defendants has been dealt with by the courts severally. Generally, in situations where the defendant is in another jurisdiction, a US court can only exercise jurisdiction by relying on the long-arm statute of relevant form or following due process under the Fourteenth Amendment of the Constitution. Under the due process requirement in the Fourteenth Amendment, general or specific jurisdiction can be exercised. In terms of general jurisdiction, the court can exercise jurisdiction over a non-resident defendant for non-forum-related activities only if the defendant's contact with the forum is "systematic" and "continuous."[189] The test for substantial contact in general jurisdiction is rigorous and to establish it, it is required that the defendant maintain substantial, continuous, and systematic contacts with the forum state before jurisdiction can be established over a non-resident defendant, even if the contact has no relation to the action in question.[190]

tracts for automatic updating from a remote facility to database held by the licencee (see s 102 UCITA).

185 See UCITA s 109(b)(1).

186 UCITA s 109(b)(2).

187 UCITA s 109(b)(3).

188 See art 15(4) UNCITRAL Model Law.

189 See the case of *International Shoe Co v Washington* 326 US 310, 316 (1945).

190 For further reading see Tang *Electronic Consumer Contracts* 108.

From the principle of establishment, the location of a server in a state is not sufficient to establish residence or systemic and continuous contact; as the location of a website could be fortuitous and can be changed. This position was upheld in *Millennium Enterprises v Millennium Music*[191] where the district court stated that it was aware of no case in which a court had asserted general jurisdiction based on the existence of an internet website. However, expressing a different opinion, the court in *Mieczkowski v Masco Corp*[192] held that general jurisdiction can be established on contacts primarily through the internet. It must be noted that in the latter case there were other traditional physical contacts besides the sole internet contact upon which the court based its findings.

Through the justice system, the US has over time developed different approaches which have been tested in different civil cases. Under the law of the Federal Circuit, the exercise of personal jurisdiction comports with the requirements of due process to the extent that a state's long-arm statute extends jurisdiction only to the limit of federal due process.[193] The Federal Circuit applies a three-part test to exercise personal jurisdiction:

(1) Defendants must have "purposefully directed (their) activities at the residents" of the forum state.
(2) The injuries for which recovery is sought must have arisen out of or is related to defendant's activities.
(3) The assertion of personal jurisdiction over defendants must comport with traditional notions of fair play and substantive justice.[194]

While establishing general jurisdiction may be rigorous, specific jurisdiction can be easily asserted over a foreign defendant where the claim is one arising out of or

191 33 F Supp 2d 907, 1999 US Dist 49.
192 997 F Supp 782 (ED Texas 1998).
193 See *Shute v Carnival Cruise Lines* 113 Wash 2d 763, 771 (P 2d 78 1989).
194 *Digital Control Inc v Boretronics Inc* 161 F supp 2d 1186 (WD Wash 2001).

relating to the defendant's forum-related activities.[195] To exercise this jurisdiction, the defendant must be engaged in acts which purposefully confer on the defendant the privilege of conducting activities within the forum state which then invokes the benefits and protection of its law. This conduct is captured in the term "purposeful availment" and requires that the defendant not only engage in activities which target the forum but does so with the intention or anticipation of targeting the forum.[196]

The various authorities on the establishment of jurisdiction in US courts on the principle of "purposeful availment" through websites or the internet are discussed below.

6.7.1 Principle of purposeful availment

The principle of purposeful availment adopted in the US to assert jurisdiction over a defendant in e-commerce cases, was founded in the case of *International Shoe v State of Washington*.[197] This case was an appeal from the Supreme Court of Washington to the Supreme Court of US challenging the imposition of a Washington State law requiring that a certain percentage of an employee's wage be paid to the state unemployment compensation fund.[198] In this case, the defendant/appellant was a Delaware corporation, with its principal place of business in St Louis, Missouri, and was engaged in the manufacture and sale of shoes and other footwear.

It maintained places of business in several states other than Washington, at which its manufacturing was carried on, and from which its merchandise was distributed interstate through several sales units or branches located outside the state of Washington. The appellant had no office in Washington and made no contracts for either the sale or purchase of merchandise there. It maintained no stock or

195 Tang *Electronic Consumer Contracts* 109.
196 Tang *Electronic Consumer Contracts* 110.
197 *International Shoe v State of Washington* 326 US 310 (1945) (hereafter *International Shoe* case).
198 *International Shoe* case 311.

merchandise in that state and made no deliveries of goods in intrastate commerce. During the years in question, the appellant had some salesmen who resided and worked in Washington. Their compensation exceeded US$ 31 000 annually.[199]
The authority of the salesmen was limited to exhibiting their samples and soliciting orders from prospective buyers at prices and terms fixed by the appellant. The merchandise was subsequently shipped free on board (FOB) to purchasers in Washington.[200] The Washington Supreme Court was of the view that the regular and systematic solicitation of orders in the state by appellant's salesmen, resulted in a continuous flow of appellant's product into the state so as to make the appellant amenable to suit in its court. The court therefore held that the fact that the corporation was engaged in interstate commerce did not relieve it of liability for payments to the state unemployment compensation fund.[201] The court held further that,

> the activities in question between the state and the corporation established sufficient contacts or ties to make it reasonable and just, and in conformity with the due process requirements of the Fourteenth Amendment, for the state to enforce an obligation arising out of such activities[202]

The Supreme Court of the US affirmed the decision of the Supreme Court of Washington.[203]

Years after this judgment, various theories or approaches have been adopted by the US courts to show "purposeful availment" in order to assert jurisdiction over a foreign defendant. This is all the more so, in cases of electronic interface where consumer cases are replete with foreign defendants. Among the theories to establish purposeful availment are the "sustained contact" test, the "sliding-scale" test, the "subject availment" test, and the "effects" test.

199 *International Shoe* case 312.
200 Ibid.
201 *International Shoe* case 315.
202 *International Shoe* case 313.
203 *International Shoe* case 322.

(a) Sustained contact test

This test postulates that the availability of web content continuously in a forum state is a "sustained contact" which is purposefully directed to the state. The basis for jurisdiction under this test is the presumption that as the web content of a corporation is accessible in a forum state, it must be available for continuous access and everyone in that jurisdiction must have or will have the opportunity to access the site. This test is simply based on access and does not apply any other criteria such as the intention of the website owner or the nature of activities of the website.

The test was established in the case of *Inset System v Instruction Set*[204] where the court asserted jurisdiction over the defendant by holding that the company's website which contained internet advertisement, was more powerful than other forms of advertisement because it was continuously accessible, and so, the court assumed, could be accessed by thousands of Connecticut residents.[205] This broad test was adopted in some subsequent cases by basing specific jurisdiction on the fact that the accessibility of the internet is a "sustained contact" which is purposefully directed to the state. The test was later criticised by some courts and, on the basis of the criticism, has largely been abandoned by the courts. One of the criticisms is found in the case of *Digital Control Inc v Boretronics Inc*[206] where the court held that the *Inset System case* represents the "outer limits" of the personal jurisdiction analysis. It held that the court jumped to the conclusion that the ready availability of the internet and its potential to reach thousands of Connecticut residents, justified the exercise of jurisdiction over the defendant, even though there was no indication that the offending website had actually been seen by a Connecticut resident, or that the defendant had engaged in any commercial activity within the forum.[207]

---

204 *Inset System v Instruction Set* 937 F Supp 161 (D Conn 1996) (hereafter *Inset System* case).

205 *Inset System* case 166.

206 *Digital Control Inc v Boretronics Inc* 161 F Supp 2d 1183 (WD Wash 2001) (hereafter the *Digital Control* case).

207 The *Digital Control* case 1186.

(b) Sliding-scale test

The sliding-scale test was established in the celebrated case of *Zippo Manufacturing Co v Zippo Dot Com.*[208] In order to confer jurisdiction, the sliding-scale test separates internet trading activities into one of three groups: a "passive website," an "interactive/intermediate website," or an "active website."

(i) Passive website

Here the defendant only makes information available over the internet for general viewing. He or she does not direct his or her activities to a specific jurisdiction or actively invite subscriptions or patronage from viewers. To the extent that the website does not enter into negotiations with consumers in a forum, personal jurisdiction cannot be exercised. In *People Solutions Inc v People Solutions Inc*,[209] the Northern District Court of Texas held that there was no purposeful availment even though the defendant had, in accordance with *Zippo*, an "interactive or middle ground" website but without repeated contacts which would justify specific personal jurisdiction.

(ii) Interactive website

A passive website can become an interactive or intermediate website by responding to consumer requests and orders in a particular forum, and exchanging information and entering into contracts with consumers in that forum. In such a case, to the extent that the website interacts with consumers in a particular forum, especially in substantial commercial communications, personal jurisdiction can be exercised. In *Clipp Designs v Tag Bags*[210] jurisdiction was established as, in addition to advertising, the defendant could also obtain orders through its website. The interactive website represents the middle-ground between passive and active websites.

(iii) Active website

Clearly, some websites are content - or commercially based with offers open to consumers without geographic limits. Such sites are involved in conscious and

208 *Zippo Manufacturing Co v Zippo Dot Com.*952 F Supp 1119 (WD Pa 1997).

209 *People Solutions Inc v People Solutions Inc*, NO CIV A. 339-CV 2339-L 2000 WL 1030619 (ND Tex).

210 *Clipp Designs v Tag Bags* 1996 F Supp 766 (ND 111 1998).

repeated transactions involving computer files over the internet. Active websites are subject to the personal jurisdiction of the forum state where the consumers are based. In *International Shoe Co v Washington,*[211] the Washington District Court confirmed that the sale of goods via an interactive website by a Missouri defendant satisfied "purposeful availment" on the basis of repeated contacts with the forums' residents.
The true test for conferring jurisdiction under the sliding-scale approach, is to consider the level of activity of the site whether it is passive, interactive, or active. To date, the "sliding- scale" test has proved useful in conferring jurisdiction in e-commerce cases.

(c) Subjective-availment test

This test relies on the subjective aim of the business itself, and not on the objective purpose shown by the website. Where it is shown that the business did not "purposefully avail" itself to the jurisdiction of the buyer, but that due to the circumstance of the sale, a buyer emerged from a different jurisdiction which was beyond the control of the seller, the consumer cannot exercise personal jurisdiction over the business. In *Winfield Collection v McCauley,*[212] the court held that the seller who sold products on auction sales on eBay did not purposefully avail herself of the privilege of doing business in Michigan, where the buyer resided. Even where it might have been foreseeable, especially at an auction sale that a consumer could emerge from anywhere, the court has held that "foreseeability alone is insufficient to support the exercise of personal jurisdiction under the federal due process clause."[213]

This test is also useful in cases of geographic restrictions for instance where a consumer bypasses the restriction by accessing the website from a different location, and then returns to the restricted location. In such a case, personal jurisdiction cannot be asserted as there has been no purposeful availment. For example, Lays Potato Chips Company in America does not sell potato chips online to consumers outside America. A Nigerian on a visit to America could order the chips and travel back to

211 *International Shoe Co v Washington* 326 US 310 (SC of US 1945).
212 *Winfield Collection v McCauley* 105 F Supp 2d 746 (ED MICH 2000).
213 See the case of *Metcalf v Lawson* 802 A 2d 1221 (NH 2002).

Nigeria to consume them. When issues arise from the purchase on opening the package in Nigeria, it would appear that the Nigerian consumer may not be able to exercise personal jurisdiction over the Lays Potato Chips Company in America.

(d) Effects test

This test looks at the effect of the act of a website on the forum which is the focal point of the activity. The *locus classicus* for this test is the libel case of *Calder v Jones*[214] where the court stated that personal jurisdiction might be appropriate if:

- the defendant committed intentional acts;
- the defendant expressly aimed his or her acts at the state; and
- the actions caused harm in that jurisdiction.[215]

6.7.2 Jurisdiction involving a non-US defendant

While the principles of internet jurisdiction especially where e-commerce is concerned, are founded in case law in the US, there is a gap where the defendant is a non-US defendant. So far, it emerges that the long-arm statute operates between states within the US and not between the US and other countries. But in e-commerce the website is open to the globe, and the question arises as to what rules will apply between a US consumer and a defendant from another country (and vice-versa). Until this question is resolved, all that the US has is a jurisdictional rule which operates within its own borders, and has limited impact on the outside community. A challenge, therefore, remains for a US consumer who may have to travel outside the US to pursue claims against foreign defendants. From the discussion above, it is submitted that internet jurisdiction is not an issue which any single nation can resolve – it transcends national boundaries and falls outside of the legislative or judicial competence of any single entity.

214 *Calder v Jones* 465 US 783 (1984) (hereafter *Calder case)*.
215 *Calder case* 788-790.

The different tests are very helpful in determining which jurisdiction will apply in e-consumer contracts. Any of the tests can be applied by the court depending on the nature of the case. However, all the tests point in one direction: the place where the business directs its activity. The one exception is the "subjective availment" test which could be applied in the case of auction sales.

It is submitted that the US purposeful-availment approach complies with international perspectives on jurisdiction over the internet. The EU Brussels Regulation allows the consumer an option to choose either to assert personal jurisdiction in the consumer's forum, or in the forum of the business. Determining jurisdiction in e-consumer contracts in the US, therefore, is well founded and recommended for international consideration.

6.8 Enforcement and implementation

Consumer protection laws are implemented in the US by the FTC. The FTC was created in 1914 to prevent unfair methods of competition in commerce. Over the years, the mandate of the FTC has been expanded to include the policing of anti-competitive practices and the administration of other consumer protection laws such as the telemarketing sales rule, the pay-per-call rule, and the Equal Credit Opportunity Act.[216] The strategic goal of the FTC is to protect the consumer and prevent fraud, deception, and unfair business practices in the marketplace. The FTC has investigative, enforcement, and administrative capacity.

Among the Bureaus under the FTC, the Bureau of Consumer Protection "may issue civil investigative demands (CIDs) to explore possible violations"[217] in the form of a subpoena. Through a CID the production of documents can be secured and witnesses can be compelled to give evidence.[218] Investigations may commence based on Presidential or Congressional requests, court referrals, consumer complaints, or

216 15 USC s 1691 1974.
217 FTC Act (1999) 15 USCA s 57b-1.
218 FTC Act s 57b-1(c)(1).

internal research.[219] Upon completion of an investigation, if the FTC has reason to believe that a violation has occurred, and that enforcement is in the public interest, it may issue a complaint to the person, partnership, or corporation in violation. A hearing is then held before an administrative law judge, and if the actions at issue are deemed a violation, the judge may recommend entry of a cease-and-desist order. If the offending party refuses to comply with the order, the FTC is authorised to approach the courts for civil penalties and restitution for the aggrieved consumer.[220] The order may be appealed to the full FTC, and from there to the Federal Appeal Court, and finally to the US Supreme Court.[221] If no appeal against the order is lodged, the order becomes final within 60 days of been issued and attracts a civil penalty of up to US$ 10 000.[222]

The FTC's mandate is carried out by seven divisions of the Bureau of Consumer Protection. These divisions address: advertising practices; financial practices; marketing practices; privacy and identity protection; planning and information; consumer and business education; and enforcement.[223] In 2009, a total of 923 054 consumer complaints were recorded.[224] To ensure further consumer protection, the FTC has a "Do-not-call Registry" where consumers of telecommunication services can register their phone lines against telemarketing which could lead to invasion of privacy on a greater or lesser scale, and an abuse of personal data through third-party collection and dissemination without consent.[225]

The FTC works for the consumer to prevent fraudulent, deceptive, and unfair business practices in the marketplace.[226] It provides information to assist consumers to spot,

219 Waller, Brady & Acosta 2011 *European Journal of Consumer Law* 4.
220 15 USCA s 5 (a)(4B).
221 15 USCA s 5(c).
222 15 USCA s 5(k).
223 See Waller, Brady and Acosta 2011 *European Journal of Consumer Law* 6-7 for more details on the various functions of the division in the area of consumer protection.
224 Waller, Brady and Acosta 2011 *European Journal of Consumer Law* 7 and in 2017 the FTC received 2.68 million consumer complaints according to the "Consumer Sentinel Network Data Book" available at https://www.consumerfinancemonitor.com (date of use: 4 October 2020).
225 FTC "Cell phones and the Do Not Call Registry" available at www.consumer.ftc.gov (date of use: 28 October 2020).
226 S 5(a) of the Federal Trade Commission Act prohibits "unfair or deceptive acts or practices in or

stop, and avoid unfair business practices. The FTC enters consumer complaints into the consumer Sentinel Network, a secure online database and investigative tool used by hundreds of civil and criminal law-enforcement agencies in US and abroad.[227] The enormous work of the FTC would make the agency appear as though it has limitless powers. There is a check however, on the work of the FTC and other government agencies by the National Small Business Ombudsman which collects comments regarding federal compliance and enforcement activities from small businesses. Each year, the ombudsman evaluates the conduct of these activities and rates each agency's responsiveness to small businesses.[228] This function of regulatory fairness by the Office of the National Ombudsman ensures a balance in the exercise of the mandate of the FTC.

6.9 Summary and conclusion

Discussing UCITA has been an extensive process. It has elaborated on several aspects of consumer transactions and provided useful insights into new ways of protecting the e-commerce consumer. The major problem with the UCITA is that it applies only to digital information and not to e-commerce goods. For the e-commerce consumer there is no distinction between goods, services, or digital information; applying the UCITA could, therefore, be confusing for the regular consumer. The UCITA has been a controversial legislation in the US[229] and in 2003 was only enacted in the states of Virginia and Maryland.[230] The UCITA has however, remained a source of analysis for courts even in states where it has not been enacted.[231]

---

affecting commerce" see UNCTAD "Consumer protection in e-commerce" 6.

227 FTC "Consumer Sentinel Network" available at https://www.ftc.gov (date of use: 28 October 2020).

228 SBA "Office of the National Ombudsman" available at https://www.sba.gov (date of use: 28 October 2020).

229 UCITA Online "The Uniform Computer Information Transactions Act (UCITA) is a proposed state contract law" available at www.ucitaonline.com (date of use: 24 October 2020).

230 Lawaspect.com "Uniform Computer Information Transactions Act (UCITA)" available at https://lawaspect.com (date of use: 24 October 2020).

231 Ibid.

The different Acts discussed in this chapter address a variety of aspects of consumer protection online. Putting all the Acts together, they are extensive, nonetheless; there remain small hiccups in providing specifically for consumer protection in the areas of: inertia selling; information requirements for sales contracts; and security of payment systems.

Of note, however, is the influence of the UNCITRAL Model Law and the EC Convention on the UETA. In the UNCITRAL Model Law ten basic international standards on e-transactions are established, namely: the legal validity of e-data and signature under articles 5 and 7; the legal validity of e-contracts and contracts by e-agents under article 11; admissibility and evidential value of electronic data under article 9; party autonomy and the incorporation of reference under articles 4 and 5*bis*; retention and attribution of electronic records under articles 10 and 13; rules on time and place of e-communication under article 15; and an eleventh principle established on the legality of e-transferable records in the UNCITRAL Model Law on E-transferable Records, 2017. All these standards are reflected in the UETA and the provisions in the UETA are on all fours with the provisions of the UNCITRAL Model Law so ensuring consumer protection under internationally-established standards. The UETA further provides for the acceptance and distribution of electronic records by government agencies in its section 17. The principle of technological neutrality in the formation and use of e-signatures is well enshrined in US law through section 102(a)(2) of the E-SIGN Act. However, what is conspicuously absent in the UETA in comparison to the EC Convention is its failure to provide mandatory information requirements for suppliers or web traders in accordance with article 7 of the EC Convention. Further, the rights of cancellation and review, and the right to performance as properly established under the EU Consumer Rights Directive are not expressly captured in the UETA, thus leaving room for disparate standards in respect of the protection of those rights.

It should be recalled that the US is a member of the OECD and is, therefore, obliged to implement the CPR. The CPR identifies the need for online disclosure in paragraph 29

and also insists on a confirmation process before consumers are compelled to maintain a transaction. Paragraph 41 of the CPR further enjoins states to facilitate safe payment systems in order to protect their citizens from fraud.[232] A review of the US laws has shown minimal compliance with any of these obligations. However, privacy, education, and awareness, together with implementation as canvassed in paragraphs 48 and 50 of the CPR, are well implemented in the US under the auspices of the FTC supported by the various bureaus set up by the Commission.

This chapter and preceding chapters have contained various principles which have been enacted in international, regional and national instruments for the purpose of protecting the rights of consumers who carry out transactions online. The next chapter which is Chapter Seven will create an opportunity to draw out the areas of similarities in these instruments and also show areas where there are core differences. These comparisons are necessary in view of the objective of the study which postulates that harmonisation will enable a better standard for the protection of e-commerce consumers.

[232] See chapter 4 para 4.2 on the principles contained in the CPR.

CHAPTER SEVEN

COMPARATIVE LAW ANALYSIS

7.1 Introduction

Internet related issues usually attracts cross border perspectives due to the borderless nature of the internet. The perspectives undertaken in this study cut across those of the UN,[1] EU and the OECD,[2] AU[3] and countries in Europe, Australia, Africa and America.[4] Each of these countries has comprehensive laws on e-commerce and these laws contain measures for the protection of the rights of consumers specific to e-transactions. In this chapter there will be a comparative study of these instruments by looking at their applications, exclusions, and level of implementation and enforcement.

7.2 Consumer protection

In applying consumer protection rules for online use some principles and rights of e-commerce consumers have been consistent in nearly all of the instruments. These principles govern information requirements; commercial communications; use of data for contract formation; limitation on the liability of ISPs; jurisdiction and the recognition of e-transferable records. While rights which are peculiar to e-commerce consumers as observed in the various instruments include rights to information; review; withdrawal; refund; delivery; privacy; and payment security. These principles and rights will be discussed in what follows.

7.3 Principles in e-transaction instruments

7.3.1 Information requirements

The bedrock for the formation of e-commerce transactions is information. Information

---

1 See Chapter 3.
2 See Chapter 4.
3 See Chapter 5.
4 These countries are Australia, South Africa, UK, and the US, Nigeria does not have an e-transaction specific legislation and is therefore not discussed under this comparative chapter.

is the first contact the consumer has with the supplier and it is the content of the information that defines the obligations in the contract. Suppliers are stringently required to state clearly the characteristics of their goods or services, all applicable costs, their contact information which should include a geographic address.[5] Suppliers are further imposed with the obligation to provide information to consumers on: interoperability of software and devices,[6] limitations on the use of digital products if any,[7] withdrawal period and processes,[8] and platforms for dispute resolution.[9] Information requirements in the EU progressively provide for the protection of users of devices with limited space for instance, those engaged in mobile commerce through regulating the means by which information will be sent to such users.[10] There is also further protection for children and vulnerable persons in the OECD by insisting on the nature of information that are suitable for such persons.[11]

7.3.2 Commercial communications

Commercial communications are generally allowed.[12] However, unsolicited commercial communications through e-mails, telemarketing, SMS and other means of e-communication are generally prohibited and could easily constitute spam; therefore obtaining consent is a prerequisite to sending commercial mails to recipients.[13] Where they are allowed they must be clearly indicated and should not be misleading.[14] Consumers should be able to opt of unsolicited commercial communications freely and

5 See CPR paras 4 &10; OECD *Toolkit for protecting digital consumers* 30; E-commerce Directive art 1(5); consumers are of necessity required to supply their information in a format that can be stored and is printable see CRD art 6; AU Convention art 2; ECTA s 43.

6 See CPR para 32; CRD art 6(1)(s); UNCTAD "Consumer protection in e-commerce" 3.

7 See CPR para 27; CRD art 6(1)(r).

8 CRD art 6(16); there are no similar provisions in the AU Convention.

9 CRD art 6(1)(t).

10 CRD art 8(4); EU DG Justice *DG Justice guidance document concerning Dir 2011/83/EU* 33.

11 CPR paras 2 & 18;

12 E-commerce Directive art 7.

13 Direct commercial communications is out-rightly prohibited under the AU Convention art 4(3); although the ETA has no prohibitive sections on unsolicited commercial communications such communications are prohibited in Australia under s 16 of the Australian Spam Act and also in the US under the CAN SPAM Act s 5(d)(2) .

14 E-commerce Directive arts 6 & 8; AU Convention art 4(5); Australian Spam Act s 17.

easily.[15] Some instruments go as far as determining a minimum period for compliance.[16] Unsolicited sales or inertia selling is generally not an acceptable means of sales. Consumers are therefore not bound to honour inertia sales and are not obliged to return such articles at their own expense.[17]

7.3.3 Use of data for electronic contracts

The use of the internet in commerce and contract formation has revolutionised the requirement of writing on paper. Of special interest is the step taken further in the EU by allowing auctions through online platforms;[18] this boost to online contracts also appears to be allowed in South Africa where however, the exercise of a cancellation or withdrawal right is inapplicable to auctions.[19] Though not specifically provided for, online auction is not prohibited under the AU Convention.[20] The retention of e-records and their attribution to the source from which they emanate are further detailed in the UNCITRAL Model Law, the ETA, ECTA and the UETA.[21] Similarly, the ETA and the ECTA reflects the principles guiding time and place of e-transactions as well as rules guiding the receipts of e-documents as provided in the UNCITRAL Model Law.[22]

7.3.4 Limitation on the liability of ISPs

In consumer contacts, the consumer enjoys a lot of protection by law as the consumer is regarded as the weaker party in a B2C contract.[23] However, the service provider who provides the platform for electronic trade is also protected from liability even

---

15 CPR para 18; Countries in EU have provision for opt-out registers see E-commerce Directive art 7. For a similar provision on opting out freely from unsolicited commercial communications see Australian Spam Act s 18; ECTA s 45, CAN SPAM Act s 5a(4)(A)(i).

16 In the US for instance, the opt–out request must be honoured within ten business days of the request, see CAN SPAM Act s 5a (4)(A)(i).

17 CRD art 27.

18 CRD recital 4.

19 See s 42(2)(b) ECTA.

20 Compare arts 2 & 6(3) AU Convention.

21 UNCITRAL Model Law arts 10 & 13; ETA ss 12 & 15; ECTA ss 16 & 25; UETA ss 12 & 9.

22 UNCITRAL Model Law arts 14-15; ETA s 14; ECTA ss 22 & 23; UETA s 15.

23 UN Guidelines for consumer protection (1999) s1.

against liability arising from consumer contracts. To enjoy this privilege the ISP must only be an access provider[24] and not the content or service provider. An ISP who acts as a supplier would be liable for any infringement or breach of contract.[25]

7.3.5 Jurisdiction

Internet transactions span across the globe without geographic limitations. The international nature of internet transaction raises issues of choice of law and jurisdiction of courts. These issues are addressed in different legal instruments in favour of the location of the consumer.[26] In Africa the AU Convention confers jurisdiction on the place where a service provider is established.[27] Australia practices a system that applies state or territorial laws, where however, the state or territorial laws are silent on a matter, the Commonwealth law applies.[28] Most countries also include a choice of law provision in their laws that states that consumers' right will not be subject to a foreign law which does not protect their rights as consumers.[29]

7.3.6 Use of electronic transferable records

An e-transferable record is an emerging area of use based on functional equivalence. Its adoption has not gained widespread recognition yet[30] but like every technological advance, its use across borders will attract its spread and create the need for a legislative update.

---

24 E-commerce Directive arts 12-13; Baistrocchi (2002) 19/3 *Computer & High Technology Law Journal* 118; Adeyemi (2018) 24/1 *Computer and Telecommunications Law Review* 9; ECTA s 73. ISPs in the US are protected under the Communications Decency Act with particular reference to s 230.

25 AU Convention art 5(6).

26 CPR para 21 expects businesses to acquaint themselves with the laws of the consumer's location; arts 18 & 19 of the Brussels Regulation confers jurisdiction on the location of the consumer. Notwithstanding, the consumer is empowered to sue the supplier in the supplier's place of business, see further Chapter 4 para 4.3.3.

27 AU Convention art 3.

28 For an overview of the Australian system see chapter 4 para 4.5; see also ETA s 15(E) & (F).

29 See for instance South Africa's ECTA s 47.

30 The provisions for e-transferable record is made by the UN in the MLER and in the US under s 16 of UETA.

7.4 Rights in context

7.4.1 Right to information

Consumers are entitled to information in respect of goods and services which they wish to acquire.[31] They should be informed of any rates or cost affecting their transaction. It is their right to have access to a supplier's contact information; terms of the contract; as well as channels of resolving disputes.[32] Terms of the contract would include prices, withdrawal processes, refund policy and privacy rules. A breach of this requirement could void a contract.[33]

7.4.2 Right to review

Before concluding a contract, consumers should be able to review the terms of the contract.[34] Consent in e-transactions should be complete and unambiguous. An exercise of the right to review or confirm a transaction helps to correct in-put errors and helps the consumer to decide on whether to continue or withdraw from a contract.[35]

7.4.3 Withdrawal right

This right is peculiar to e-commerce consumers. In conventional trade the catch word is "buyers beware" this is however not the case in e-transactions as buyers are not able to inspect goods or services before concluding the contract. The withdrawal right

---

31 OECD "Improving online disclosures" 2,5; see also OECD *Consumer education* 6.

32 E-commerce Directive art 10 provides further for contract terms to be in forms that eases stor age and reproduction; see further Hathaway and Savage "Duties for internet service providers" 4 on the need for suppliers to meet their obligations in order to avoid cancellations.

33 Vagadia "Contract discharge and methods to reduce liability" 74. Ordinarily a consumer should give a supplier notice of withdrawal from a transaction within 14 days of concluding a transaction where however, the supplier fails to inform the consumer of his/her right to withdraw from a contract this withdrawal period extends to 12 months after the initial 14 days or 14 days from when the supplier eventually informs the consumer of his/her withdrawal rights during the 12 months period CRD art 10.

34 CPR para 38; E-commerce Directive art 11(2); CRD art 8(7); AU Convention art 5(3).

35 OECD *Toolkit for protecting digital consumers* 35; UETA s 10.

opens a window to close the gap between conventional consumers and e-commerce consumers by allowing the e-commerce consumer to withdraw from a contract without reason and during a cooling off period.[36] For contracts that are on a going basis or renewable, consumers' right to opt out or withdraw from such contracts should be maintained by suppliers.[37]

7.4.4 Right to refund and cancellation

Where a consumer has made payment in respect of a transaction he or she is entitled to a refund in the event of cancellation or withdrawal.[38] Most legislation details that the refund would be through the same means of payment[39] and where the goods are returned the consumer will be responsible for the cost of return.[40] Services which have begun before cancellation will be paid for according to the transaction which has already been performed.[41] The CRD and the ECTA takes the rule further by providing a time frame for refund.[42] It must be noted that not all contracts for goods or services can be cancelled. Cancellation does not extend to personalised goods or services, or to goods that expire, deteriorates or becomes unhealthy when its seal is broken, contract for services that has been fully performed, or which begun with the consumer's consent. Contracts for the supply of goods or services which fluctuates, contracts for supply of newspapers, periodicals, or magazines as well as contracts at public auctions cannot be cancelled.[43]

---

36 CPR para 19; OECD *Toolkit for protecting digital consumers* 35. The cooling off period for the exercise of a withdrawal right is 14 days in the EU see CRD art 9 see also European Parliament *Towards new rules* 7. In South Africa the cooling-off period is within 7 days see ECTA s44.

37 OECD "Consumer policy guidance on intangible digital content" 15.

38 European Parliament "Towards new rules" 7; CRD art 13

39 CRD art 13.

40 CRD art 14(1). This same article provides that the consumer should return the goods within 14 days of sending his/her withdrawal notice. The burden of proof showing that a proper withdrawal process was followed lies on the consumer see CRD art 11(4).

41 CRD art 13(3); furthermore, art 13(3) permits the supplier to hold unto refunds until such goods which are meant to be returned are recovered or evidence of return is shown. The ETA and AU Convention do not contain similar provisions.

42 In the EU refund should be made within 14 days of receipt of a withdrawal notice see CRD art 13. The refund period is also within 30 days in South Africa see ECTA s44 (4). There is no provision for a refund process under the AU Convention.

43 CRD art 16; ECTA s 42(2). There are no similar provisions in the US or Australia.

7.4.5 Right to timely delivery

One of the earlier inhibitions in online trade was consumers' fear of a faceless transaction especially in the occurrence of non-performance. Goods and services are required to be delivered within a reasonable time after the conclusion of a contract and for some jurisdictions the time frame is 30 days.[44] A transaction can be cancelled due to delay in performance especially when performance is expected within a specified time frame or within a "reasonable" time.[45] It is submitted that a specified time frame is more definite than the option of a "reasonable" time since reasonableness is a subjective opinion.

7.4.6 Right to payment security

Online payment is an integral part of e-commerce. It gives beauty to digital trade as consumers are able to begin and conclude a transaction seamlessly. Through the payment gateway a lot of security issues come to play. Suppliers are obligated to provide authentication and security on their payment platforms before enabling fund transfer otherwise consumers' interest will be compromised.[46] It is therefore a consumer's entitlement to utilise platforms that are safe while the supplier is duty bound to provide a secured payment system.[47] Consumers should also be able to retain payment or transaction information on their e-mails or other durable media.[48]

7.4.7 Access to dispute resolution

The essence of law is to ensure justice. E-commerce most often involves trans-border trade and suffers the challenges of distance, choice of law, jurisdiction and enforcement of judgement. Access to justice is a fundamental right and this can hardly be attained in e-commerce transactions in the absence of a Convention which binds

44 CRD art 18(1); ECTA s 46(1).
45 CRD art 18(2); ECTA s 46(2).
46 UNCTAD "Consumer protection in e-commerce" 7.
47 CPR para 40; ECTA s 43(5).
48 OECD "Consumer policy guidance" 7.

everywhere the internet can be accessed. Dispute resolution online or conventionally through mediation channels, help-desks and settlement houses will help to eliminate the challenges of resolving trans-border cases in court.[49]

7.5 Exclusions

Through the entire legislative texts some items were generally excluded from the application of e-commerce consumer protection laws. These items include C2C transactions;[50] B2B transactions;[51] taxation; the provision of offline services; gambling activities; [52] employment relationships; non-electronic activities such as auditing; litigation; notarization;[53] agreements on cartel law; and medical advice which is of a non-general nature.[54]

Contracts that create or transfer rights in real estate,[55] except for rental rights; requires the involvement of courts; public authorities or professions exercising public authority; contracts of suretyship and collateral securities by consumers as well as contracts governed by family law or the law of succession such as wills are generally excluded from e-transaction and consumer protection laws.[56]

---

49 CPR paras 35 & 46.

50 E-commerce Directive recital 18; in contrast C2C transaction is protected in OCED member states with reference to the Preamble of the CPR.

51 B2B transactions are however, envisaged under the AU Convention see art 5.

52 The exclusion of gambling activities does not include promotional competitions or games where The purpose is to encourage the sale of goods or services and where payments are only meant to secure the promoted goods or services, see AU Convention art 2.

53 AU Convention art 2.

54 E-commerce Directive art 1(5); CRD art 3, the CRD further excludes contracts for the single use of an internet connection.

55 Contracts on immovable properties are not considered as consumer contracts that should be captured under e-transactions see Cauffman (2012) 19/1 *Maastricht Journal of European and Comparative Law* 213-214.

56 E-commerce Directive art 9; UETA s 3.

7.6 Conclusion

The exposition in this chapter draws out similar levels of recognition and enforcement of electronic communication in transactions across borders. Similar exceptions were also observed especially in the execution of private family deeds and succession. Some areas of consumer protection, however, did not enjoy widespread recognition as they were either not provided for in entirety in some laws or that their level of protection varied from one law to the other.

Nevertheless, the experiences of the EU are predictably more far-reaching in view of the greater influence of the electronic media in the European community. From a comparable point of view the different principles adopted by the EU could be said to be adequate for protecting e-commerce consumers. Lessons learnt from the EU legal reform hinges on full harmonisation.[57] Until other regions in the world are able to take the initiative and secure a fully harmonised framework for e-transactions within their regions, comprehensive e-commerce consumer protection may remain a mirage.

Apart from the enactment of consumer protection policies, the bane of internet trade has been the undefined system for implementing orders or judgement in cross-border consumer issues. Paragraph six of the Consumer Protection Guidelines of the OECD presents a positive step towards addressing the challenge of implementation.[58] Suffice it to point out that the recommendations on redress as contained in paragraph 7 of the CPR have been largely achieved in nearly all OECD states.[59]

Although UK regulations were not particularly referred to in this chapter, it is worth mentioning that the UK regulations on e-commerce and consumer protection successfully implement the provisions of the EU Directives in UK national legislation.

---

57 See Chapter 3 para 4.5.1 on the full harmonisation principle in the CRD.

58 Future work on consumer redress which provides more detailed principles can be found in OECD Consumer Dispute Resolution and Redress Recommendation.

59 OECD *Consumer protection enforcement* 5.

For comparative purposes, the legal framework of the Australian continent was also studied and putting together the pieces of Australian legislation on e-commerce, it can be concluded that the ETA which is the main legislation on e-commerce and consumer protection in Australia is modelled after the UNCITRAL Model Law and is not influenced by the EU Directives under study. The ETA glaringly falls short of the basic protective measures contained in the CRD.

E-commerce consumers in the US are protected within state and federal laws. Due to the ubiquitous nature of the internet, most of the laws bordering on e-commerce consumers are the enactments of the ULC. The UETA and the CAN-SPAM Act for instance are federal enactments and they sufficiently provide adequate protection for consumers within the US. The UETA is comprehensive and adopts most of the principles contained in the UNCITRAL Model Law. Several cases have been tried in the US on jurisdiction and unfair terms and these cases are consistent in protecting the rights of e-commerce consumers.[60]

With reference to Africa, although the AU Convention on Cyber Security and Personal Data Protection contain some measures for the protection of consumers, the level of protection is minimal and inadequate.[61] It falls far short of existing frameworks for consumer protection in jurisdictions which already have regional and national legislation on e-commerce. This observation notwithstanding, a review of the South African ECTA brings to bear the influence of the UNCITRAL Model Law as well as that of the CRD on the South African legal framework for e-commerce and the protection of e-commerce consumers. The ECTA appears more protective than the AU Convention and would therefore serve as a good model for Africa.

---

60 See Chapter 6 particularly paras 6.6.5 & 6.6.6.

61 The AU Convention has a total of 14 signatures and 5 ratifications. Nigeria and South Africa, which are the African countries elected for this study are yet to ratify the Convention. The Convention is not yet in effect based on the provision of art 36 which provides that the "Convention shall enter into force thirty (30) days after the date of receipt…of the fifteenth (15th) instrument of ratification."

Chapter 8 of this study is an examination of the existing regulatory framework for the protection of e-commerce consumers under a jurisdiction with no legislation that specifically addresses e-commerce and the protection of e-commerce consumers.

CHAPTER EIGHT

THE IMPACT OF NIGERIAN LEGISLATION ON ELECTRONIC COMMERCE CONSUMERS

8.1 Introduction

The essence of the study in this chapter is an evaluation of the level of protection which is available to e-commerce consumers in the absence of an e-transaction-specific legislation. To achieve this, the relevant laws on consumer protection in Nigeria are examined, and their provisions contextualised for consumers who do business, online.

Consumer protection has an age-old legal tradition that exists at various levels around the world. In some countries it is actively pursued and thus effective, while in others, consumer - protection principles exist only in textbooks in which the fundamental objective of a "good buy" is seen as the cardinal responsibility of the buyer under the popular maxim *caveat emptor*. Nigeria is no different from the norm as consumer protection is not effectively pursued.[1] And this has led to an ineffective consumer protection regime in Nigeria with dire consequences, especially for consumers of electronically acquired goods and services. There are instances where offers have been made to subscribers without opt-out options, and where m-consumers have been made to pay for services to which they have not subscribed.[2]

Nigeria is a huge consumer of e-goods and services, as of 9 February 2018 the Nigerian Communications Commission (NCC)[3] issued a figure of 98.3 million internet users in Nigeria.[4] This accounts for a large per cent of internet use in the world, either as consumers or suppliers, but these users operate without a regulatory framework.

1 Eseyin and Chukwuemeka (2018) 72 *Journal of Law, Policy and Globalization* 125.
2 Akhigbe (2019) *6 Benin Journal of Public Law* 201.
3 Nigerian Communications Act, 2015.
4 NCC "Internet users in Nigeria hit 98.3 million" December 2018 available at www.ncc.gov.ng/thecommunicator/index (date of use: 15 October 2020).

Nigeria is also recognised within the African continent for its high mobile money deployments, through the use of mobile phones for e-transactions.[5] While consumer distress may be a domestic problem in Nigeria, the international dimension of e-commerce has made it necessary for Nigeria, like most other countries in the world, to awake to the responsibility of providing legal protection for all forms of consumers, especially at a level that meets international standards.

To facilitate the use of information technology in Nigeria in 2007, the National Information Technology Development Agency (NITDA) was established.[6] The primary function of the Agency is to plan, develop, and promote the use of information technology in Nigeria. That mandate is, however, unattainable without legislation governing e-transactions. Since 2009, there have been efforts to legislate on e-transactions. The first e-transactions Bill was the Electronic Communication and Transactions Bill 2009; followed by a Bill for the Prohibition of and Punishment for Electronic Fraud and Crime in all Electronic Transactions in Nigeria and other Related Matters, 2011; and then the current Bill, which is a Bill for an Act to Facilitate the Use of Information in Electronic Form for Conducting Transactions in Nigeria and for Connected Purposes, 2017 (E-transactions Bill).[7] Apart from the E-transactions Bill, there are fragmented conventional laws which provide some measure of protection for consumers. These laws are evaluated in terms of their adequacy and adaptability to address changes peculiar to the electronic environment.

Sources of law in Nigeria are primarily customary law, common law, equity; legislation; and case law. Of these, legislation is the fundamental law of the land drawing strength from the basic norm which is the Constitution of the Federal Republic of Nigeria.[8] In essence, common law, judicial decisions, and legislation form the bedrock for legal

5 UNCTAD *Review of e-commerce legislation* 2; in 2015 mobile penetration in Nigeria was said to be about 108 per 100 inhabitants, International Trade Center "International e-commerce in Africa" 6.

6 National Information Technology Development Agency Act, 2007.

7 The Bill passed its second reading in 2013, and in 2017 it passed the third and final reading and is now ready for Presidential assent, see NASS "Votes and proceedings" available at www.nassnig.org (date of use: 20 June 2020).

8 Constitution of the Federal Republic of Nigeria, 1999 (amended 2011).

protection and redress against undesirable practices, trespass, and infringements arising from torts and contract.[9]

A discussion of Nigerian law would be incomplete without reference to its origin. The establishment of English rule in Nigeria led to the adoption of English law prior to attaining independence in 1960, and assuming the status of a Republic in 1963. In 1861, Lagos was ceded to the British Crown and British common law and equity began to be applied in Lagos. In 1876, section 14 of the 1876 Supreme Court Ordinance took effect. It provided that "the common law, the doctrines of equity, and the statutes of general application which were in force in England on the 24th day of July, 1874, shall be in force within the jurisdiction of the Court." In 1902, a similar proclamation was enacted for the Northern region of Nigeria,[10] and with the unification of the Northern and Southern Nigerian Protectorates in 1914, a further Supreme Court Ordinance was promulgated which incorporated all English law applicable in England from 1900 into Nigerian law.[11]

The earliest of consumer-related laws during that period dealt with competition and the protection of consumers from harmful products. Consumer protection, if any, was only a part of existing measures and did not specifically address consumer protection as such.[12] In Nigeria, a law that could be readily referred to for consumer protection was one of the received English laws: the Sale of Goods Act of 1893. Nigeria continued applying the received English laws until 1963, when she became a Republic. As a Republic, although Nigeria enacted her own laws, most of these were modeled on their English counterparts – the title of the law may have changed; however, the letters of the law remained.

9 Elegido *Jurisprudence* 244, 269.
10 Ikhide *Consumer Protection Law* 4.
11 Supreme Court Ordinance 1914 s 14.
12 Ndubuisi, Anyanwu and Nwankwo (2016) 6/4 *Arabian Journal of Business and Management Review* 2.

8.1.2 Regulatory framework

The regulatory framework for consumer protection in Nigeria is currently made up of the Trade Malpractices (Miscellaneous Offences) Decree, 1992; the National Agency for Food and Drug Administration and Control Act (amended) Decree 15 of 1993 (NAFDAC);[13] the Standards Organisation of Nigeria Act, 2015;[14] and the Federal Competition and Consumer Protection Act, 2019 (FCCPA).[15] The FCCPA is the principal legislation governing consumer protection in Nigeria. The framework is further strengthened by the Nigerian Communications Act, 2003;[16] the Nigerian Communications Commission (Registration of Telephone Subscribers) Regulations, 2011;[17] and the Cybercrimes (Prohibition, Prevention, etc) Act, 2015.[18]

Although these Acts are related to consumer protection, not all of them impact directly on the consumer, as certain of the Acts are advisory in nature and recommend standards for relevant government sectors on policies, directions, and means of safeguarding the health and interest of consumers. The FCCPA, the Nigerian Communications Act, the NAFDAC Act, and the CPC Act, however, impact directly on consumer protection. In fact, the Federal Competition and Consumer Commission created by the FCCPA, provide means by which consumers may directly access its services and seek redress. And the Cybercrimes Prohibition Act, being more recent and an internet-related legislation touches on very important areas in safeguarding the interests of consumers who carry out transactions online.

13 NAFDAC Act, 1993, codified in Laws Federation of Nigeria (LFN) Chapter N1 2004.
14 Standards Organisation of Nigeria Act, 2015.
15 Federal Competition and Consumer Protection Act 2019.
16 Nigerian Communications Act, 2003 (Act No 19 FRN Official Gazette Vol 90, 19th August, 2003).
17 Nigerian Communications Commission (Registration of Telephone Subscribers) Regulations, 2011 (FRN Official Gazette Vol 98 7th November, 2011).
18 Cybercrimes (Prohibition, Prevention, etc) Act, 2015.

8.1.2.1 Trade Malpractices (Miscellaneous Offences) Decree 1992

The Decree prohibits misleading advertising; false or unjust measures or measuring instrument or instruments that are not stamped in accordance with the provisions of the Weights and Measures Act.[19]

The reality, however, is that as with most consumer protection laws, there are hardly any reported cases invoking the protection of an Act such as the Weights and Measures Act because of the lengthy processes involved in litigation, and the absence of effective and popular consumer- protection redress centres in the country. Besides that, the provisions of the Act are not applicable to online marketing and misleading advertisement on the internet.

8.1.2.2 National Agency for Food and Drug Administration and Control Act, 1993 (amended)

The National Agency for Food and Drug Administration and Control (NAFDAC) was created in 1993 under the NAFDAC Act.[20] One of the primary functions of the Agency is to regulate and control the importation, export, manufacturing, advertisement, distribution, sale, and use of food, drugs, cosmetics, medical devices, bottled water, and chemicals.[21] The NAFDAC is an agency of the Federal Ministry of Health established to "…give a frontal attack to health problems arising from foods, chemicals, drugs, medicines and similar regulated products without the inhibitions of the civil service settings."[22] The Agency is empowered to enter premises, seize any material for inspection or laboratory testing, and detain, or if necessary destroy, dangerous drugs or food.[23]

19 Trade Malpractices Decree ss 1 and 6.
20 NAFDAC Act s 1.
21 NAFDAC Act s 5.
22 NAFDAC *Panoramic Report of Activities and Achievements*, 1994-2000.
23 NAFDAC Act s 24.

Today in Nigeria, assessing whether drugs are controlled, or are original or a counterfeit, is very easy and cost free. All that is required is for the consumer to scratch a panel on the drug packaging and send the PIN through free SMS to 38353 or call a predetermined number before purchase. In a few seconds, a response from that number indicates whether the drug is fit for use or not. Where the drug is not fit for use, it is the duty of the consumer to give further information to the Agency to enable it to locate the pharmaceutical shop or chemist for further investigation.

It is an offence to process or sell food, water, or drugs that have no NAFDAC approval. It is also an offence to obstruct an officer of the Agency from the lawful discharge of his or her duties. The offence attracts a fine of ₦5 000 (five thousand naira) or two years imprisonment, or both fine and imprisonment.[24]

Offences under the NAFDAC Act are not taken lightly. In 2008 Barewa Pharmaceuticals Limited[25] produced a teething powder which led to the death of a number of children. The company was fined the sum of ₦1 00 000 (one million naira) at the Appeal Court and this was upheld by the Supreme Court.[26] As can be observed this law does not provide protection for e-commerce consumers whose purchases online may be delivered as cloned or defective goods or services that are not functional.

8.1.2.3 Standards Organisation of Nigeria Act 2015

The Standards Organisation of Nigeria (SON) was established in 1971 and was designed to form an integral part of the Federal Ministry of Industries until the 2004 amendment which made it a body corporate. The SON Act S9 2004 was however repealed and replaced by the SON Act, 2015.[27]

---

24 NAFDAC Act s 25.

25 *Barewa Pharmaceuticals Limited v FRN* (unreported) Suit No SC.530/2016 judgment delivered on 12 April 2019 (hereafter the *Barewa* case).

26 The *Barewa* case para 60.

27 Repealed in s 50 of the Standard Organisation of Nigeria Act, 2015.

The functions of the organisation are outlined in section 5 of the SON Act and includes the powers to ensure that standards are complied with.[28] The organisation also has powers to undertake, investigate as necessary, the quality of facilities, materials, and products. Products that meet the quality-assurance test are usually awarded the Nigerian Industrial Standard (NIS) certification mark.[29] The object of this mark is to give consumers a sign to look out for when making purchases. But the Nigerian market is so large and, in the main, unenlightened, that most consumers are not aware of the NIS certification. This results in purchases without reference to the NIS mark which totally erodes the objectives of the organisation. The principal limitation facing the SON is its inability to police the Nigeria market in which "kitchen manufacturers"[30] affix the NIS certification mark to their products to mislead unwary consumers. Manufacturers who engage in such deceptive practices are, however, committing an offence which is punishable under the SON Act.

To advance the functions of SON, the Standards Organisation of Nigeria Conformity Assessment Programme (SONCAP) was established in 2005 to help ensure that products exported to Nigeria are safe for consumers. The SONCAP is a product-conformity scheme which assesses and verifies regulated products, including: toys; automobiles; used products (other than automobiles); chemicals, electrical and electronic products.[31]

8.1.2.4 Federal Competition and Consumer Protection Act 2019

The FCCPA is the current legislation on consumer protection in Nigeria. It replaces the Consumer Protection Council Act of 2002 (CPCA) which was a direct legislation on consumer protection. The CPCA was revised and passed by Senate on the 8 of June

28 Consumer Awareness Organisation *Research report* 56.

29 SON Act s 10; see also Inegbedion (2010) 2 *Justice* 38.

30 The term "kitchen manufacturers" is descriptive of the mode of production of micro-mini and home industries where products are manufactured and produced for the market without going through the formalities of registration, accreditation and standardisation.

31 Intertek "Information for importers" available at www.exports2nigeria.com (date of use: 23 October 2020); see also https://son.gov.ng (date of use: 23 October 2020).

2017 as the Federal Competition and Consumer Protection Bill 2016 (FCCP Bill);[32] while awaiting presidential assent the Bill was further revised and reconsidered by the National Assembly. The revised Bill was passed by the National Assembly on 5 December 2018[33] and got presidential assent on 7 February 2019. The FCCPA applies to all commercial entities in Nigeria including government institutions[34] and provides for a Competition and Consumer Protection Tribunal.[35] The tribunal has jurisdiction over appeals from decisions of the Commission. Should a consumer be dissatisfied with the decision of the tribunal he or she may appeal to the Court of Appeal.[36]

A wide range of consumers' rights are protected by the mandatory requirements that suppliers provide clear and accurate information and make necessary disclosures to consumers.[37] Consumers have rights to information; cancellation; return of goods and protection from unfair trade terms and practices, misrepresentation and unfair contract terms.[38] A breach of any of the rights of consumers as outlined in the FCCPA attracts punishment under its s 155. The clear inclusion of these rights in the FCCPA improves greatly on the CPCA which hitherto did not directly outline rights which it sought to protect. The FCCPA is very wide and takes into consideration other aspects of trade that impact on the interest of consumers besides safeguarding their rights. These aspects include competition; monopoly; price regulation; and mergers. In the exercise of the functions of the Commission, it may make regulations to prescribe procedures, administrative penalties and fees.[39] An evaluation of the FCCPA will however, be limited to the scope of this study in line with examining the rights of consumers within the objectives of consumer protection.

32 Placng "Senate passes Federal Competition and Consumer Protection Bill" 08 June 2017 available at https://placng.org/home (date of use: 02 October 2020).
33 Agbajileke "Senate Reconsiders Passes Federal Competition and Consumer Protection Bill" available at www.businessdayonline.com/05 December 2018 (date of use 05 October 2020).
34 FCCPA s 2.
35 FCCPA s 39.
36 FCCPA s 103.
37 FCCPA ss 114-133.
38 Ibid.
39 FCCPA s 163.

The rights now enshrined in the FCCPA are elaborate and a clarification of who enjoys legislative protection as a consumer becomes necessary. The FCCPA defines a consumer as a "person who purchases goods, pays for or subscribes to services other than for commercial purposes."[40] The FCCPA further defines a person as a natural or legal person who may be incorporated or not. This definition extends consumer protection in Nigeria to both natural and juristic persons who make purchases or pay for services for non-commercial use.[41]

The rights of consumers under the FCCPA are protected through the functions of the Federal Competition and Consumer Protection Commission which is created under section 3 of the FCCPA. Their functions are to administer and enforce the provisions of their enabling law; resolve consumer disputes and apply appropriate sanctions, where necessary.[42] They are also empowered to register all imported goods for the purpose of traceability.[43] The Commission is further mandated to police the safe and qualitative delivery of services by service providers amongst other functions.[44] In the exercise of these functions, the Commission may summon witnesses, have them examined, administer oaths, call for verification of documents, make prohibitive orders, demands, and can go as far as sealing up premises.[45] Consumers may enforce their rights or seek to resolve any dispute by making direct complaints to the service provider, industry regulator, the Commission or a court with competent jurisdiction.[46]

Manufacturers and suppliers are mandated to label their products with their contact details otherwise they would be guilty of an offence.[47] And where a consumer suffers loss or harm arising from the use of a product, he or she will be entitled to compensation. Natural persons are liable on conviction to a fine not exceeding ₦10

40 FCCPA s 167.
41 Ibid.
42 FCCPA s 17(h).
43 FCCPA s 17(q).
44 FCCPA s 17(y).
45 FCCPA ss 17-18.
46 FCCPA s 146.
47 FCCPA s 134.

000 000 (ten million naira) or a maximum of 3 years in prison or both. While corporate bodies "shall be liable on conviction to a fine not exceeding ten percent of its turnover in the preceding year."[48] This provision of the FCCPA serves two purposes first, it prohibits anonymity and secondly, it punishes manufacturers and suppliers for the sale of harmful products.

The FCCPA contains a very important section that is outreaching; section 104 makes every other law on competition and consumer protection subject to the FCCPA the only exception being the Constitution of the Federal Republic of Nigeria.

The bane of consumer protection in Nigeria was lack of awareness of the existence of the Consumer Committee and its functions under the CPCA. This can, in essence, be laid at the door of the Committee's ineffectiveness. Now it is expected that with an improved legislation as the FCCPA, consumers will be better protected. The powers of the Commission are wide and if effectively applied, consumers who transact offline will be highly protected. However, as with most consumer protection laws, there are no specific provisions that are capable of addressing issues which are peculiar to online transactions such as interoperability and information for buyers of digital products or licences; amongst others. In addition to the Cybercrimes prohibition Act, the FCCPA is a very strong tool for consumer protection in Nigeria having repealed the age long CPCA.[49]

8.1.2.5 Nigerian Communications Act 2003

The Nigerian Communications Act (NCA) applies to the provision and use of all communications services and networks and seeks to protect the rights of service providers and consumers within Nigeria.[50] It establishes the Nigeria Communications Commission whose responsibilities include granting and renewing communication licences and the promotion of fair competition among communication services and

48 FCCPA s 135.
49 FCCPA s 166.
50 NCA s 1(g).

facility providers.[51] The legislation is more focused on the management of communication services than on consumers.

Nonetheless, complaints against service providers may be sent to the Commission as provided in section 62, and the Commission is under an obligation to address the complaints within 60 days and report its decision to the parties involved on whether or not to investigate. Under the NCA service providers are under an obligation to provide quality services to consumers.[52] For its part, the Commission is obliged to preserve consumers' information through the designation of a consumer code agency.[53] They are also to protect consumers from undue advantage by subjecting tariff rates by service providers to the prior approval of the Commission.[54] Consumers are further afforded access to the Commission's Register in physical and electronic form, this Register is maintained by the Commission and it contains information on all matters falling within the NCA.[55] Finally, the Commission is empowered to resolve consumer disputes and fine offenders,[56] while the Federal High Court has exclusive jurisdiction over matters involving the Commission.[57] In essence, the relevance of the NCA to consumer protection is its pivotal role in resolving consumer complaints regarding the quality of the services rendered by service providers; providing access to information regarding service providers whose information are contained in the Register; and resolving other general complaints.

In terms of section 70 of the NCA, the Nigeria Communications Commission (Registration of Telephone Subscribers) Regulations, 2011 (NCC Subscriber Regulations), have been issued. The NCC Subscriber Regulations provide for control of the subscription database and the registration of mobile telephone subscribers[58]

51 NCA s 4.
52 NCA s 104.
53 NCA s 106.
54 NCA s 108.
55 NCA ss 68 and 69.
56 NCA ss 104 and 111.
57 NCA s 138.
58 NCC Subscribers Regulations reg 2

including information of foreign licencees on the network of a licencee in Nigeria.[59] The central database is restricted and only made available to licencees upon agreed terms.[60] Senior security officers may also access subscriber information on the database upon a written request which must be for security purposes,[61] provided the release of the information is lawful.[62] Subscribers are at liberty to request their personal information and update it.[63] Registration of subscribers' information is mandatory and this database has been helpful to consumers in Nigeria, especially in the detection of fraud and other criminal activities by revealing the identities of previously anonymous subscribers.[64]

8.1.2.6 Cybercrimes (Prohibition, Prevention, etc) Act 2015

The Cybercrimes (Prohibition, Prevention, etc) Act, 2015 (CPP Act):

> provides an effective, unified, and comprehensive legal regulatory and institutional framework for the prohibition, prevention, detection, prosecution, and punishment of cybercrimes in Nigeria. The CPP Act also ensures the protection of critical national information infrastructure, and promotes cybersecurity and the protection of computer systems and networks, electronic communications, data, and computer programmes, intellectual property, and privacy rights.[65]

Although, on cybercrime, the interesting aspect of the CPP Act relevant to this study is that it promotes e-communications, prohibits spamming and phishing, ensures performance, and protects data and payment systems. The provisions further protect consumers from misleading trade practices and fraud through the prohibition of identity theft, cybersquatting, and the infringement of trade marks. It is critical to note that within the meaning of the CPP Act, a consumer includes organisations.[66]

---

59 NCC Subscribers Regulations reg 3.
60 NCC Subscribers Regulations reg 7.
61 NCC Subscribers Regulations reg 8.
62 NCC Subscribers Regulations reg 10(2).
63 NCC Subscribers Regulations reg 9.
64 The NCC fined telecommunications operators who allowed subscribers to use their services without proper registration. "Telecom giant MTN Nigeria has been fined a record 5.2bn by Nigeria's Communications Commission (NCC). MTN was fined for non-compliance with a deadline set by the NCC to disconnect all non-registered sim cards…" available at https://www.bbc.com/news 26 October 2015 (date of use: 22 October 2020).
65 CPP Act, Explanatory Memorandum.
66 CPP Act s 58.

These provisions are considered below:

(a) Promotion of e-communication

In section 17, the CPP Act provides that the use of an e-signature is binding on any contract. The burden of proving a signature rests on the party claiming the veracity of the signature. It is criminal to forge a person's signature, and forgery attracts seven years' imprisonment or the payment of a fine not exceeding ₦10 000 000 (ten million naira) or both fine and imprisonment. Service providers are under an obligation to retain prescribed traffic data[67] for at least two years, and must take steps to protect the data.[68] Such data may only be accessed by an order of court.[69]

(b) Prohibition on spamming, phishing, identity theft, cybersquatting, and the infringement of trademarks

The prohibition on the offences of spamming, phishing, identity theft, cybersquatting, and the infringement of trademarks has a direct impact on consumer protection. Spamming could amount to a waste of the consumer's resources in attempting to delete or opt-out of such messages; it could also be dangerous where the spam is virus infected. On the other hand, by phishing, sensitive information can be fraudulently acquired through mails by misrepresenting an institution and requesting a user name or change of password. The CPP Act prohibits spamming and phishing with a fine of ₦1 000 000 (one million naira) or three years' imprisonment or both.[70] Identity theft is the theft of another person's "personal information to obtain goods and services through e-based transactions", and attracts a punishment of ₦7 000 000 (seven million naira) or five years' in prison, or both.[71] Besides phishing consumers can be misled to transact with cyber squatters who operate with misleading domain names. Consumers may also divulge sensitive information while on the site and this information could

67 Traffic data means any computer data relating to a communication by means of a computer sys tem or network, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service; CPP Act s 58.

68 CPP Act s 38.

69 CPP Act s 39.

70 CPP Act s 32.

71 CPP Act s 22.

subsequently be used by the squatters to defraud the unwary consumer. The CPP Act attaches a penalty of ₦5 000 000 (five million naira) or two years' imprisonment, or both, to the offence of cyber-squatting.[72]

(c) Performance

The CPP Act ensures performance in e-transactions by criminalising non-performance. An operator of a website or creditor who deliberately fails to perform his or her part of a contract could be fined up to ₦1 000 000 (one million naira) or face imprisonment for three years, or both.[73]

(d) Protection of payment systems and data protection

One of the critical measures used by the CPP Act to protect the payment system is the protection of consumers from fraudulent use of their financial information. The act of obtaining information or details of a cardholder by any means with an intent to defraud is a punishable offence and attracts imprisonment for a period of three years or a fine of ₦1, 000,000 (one million naira) or both.[74] The sale of card holders' information such as their names, addresses, and account numbers to third parties is prohibited and punishable with a fine of ₦10 000 000 (ten million naira).[75] The deliberate or intentional issue of false payment instructions by any staff of a financial institution is also an offence and attracts imprisonment for seven years.[76] The same applies to the fraudulent re-direction of fund-transfer information during transmissions.[77] The unauthorised and intentional forgery or use of a consumer's code or information by a vendor or service provider for any gain, is punishable under the CPP Act with a fine of ₦5 000 000 (five million naira).[78] In the same way, accessing credit cards or other devices to obtain cash, credit, goods, or services is an offence that attracts

72 CPP Act s 25.
73 CPP Act s 33(8)(b).
74 CPP Act s 36(1).
75 CPP Act s 33(12).
76 CPP Act s 20.
77 CPP Act s 36(2).
78 CPP Act s 33(1).

imprisonment for seven years or a payment of fine of ₦5 000 000 (five million naira), or both.[79]

Having evaluated laws relating to e-commerce and e-commerce consumer protection in Nigeria it falls to reason that these laws definitely did not envisage protecting consumers involved in e-transactions. In the paragraph below, a further attempt will be made to streamline issues that are peculiar to cyberspace and apply extant laws to resolve those issues. The objective of this approach is to explore the possibilities of e-commerce consumer protection and the regulation of e-commerce by conventional consumer protection laws.

`8.2 Legal validity of electronic transactions and the protection of electronic commerce consumers under Nigerian legislation

For the attainment of consumer protection and the enforcement of consumer rights the responsible organ is the Federal Competition and Consumer Protection Commission. However, the text of the FCCPA is incapable of extending proper consumer protection to the online space. The legal validity of data messages was unknown to Nigerian law until the advent of the current Evidence Act[80] which, for the first time, validated e-communications. Under the new Evidence Act, relevant sections lend support to the use of data communications in consumer contracts.

In the paragraphs below, the Evidence Act and certain laws on contract will be considered to establish the level of protection they offer to online consumer transactions in terms of the following:

(a) The legal recognition and evidential weight of data messages and electronic signatures.

(b) Formalities in e-contracts.

(c) Legal protection for e-payment systems.

79 Ibid.
80 Evidence Act, LFN 2011.

(d) Consumer protection and information requirements.

8.2.1 The legal recognition and evidential weight of data messages and electronic signatures

A valid agreement must reflect the meeting of minds[81] and this can be evidenced in writing or inferred from the conduct of the parties. The requirement of writing is complemented by a further requirement of signature, which goes to show the intention of the maker to identify him - or herself as the maker of that document and to be bound by it. Where transactions are carried out electronically, the information that reflects such a transaction is represented electronically either in soft copy, or reproduced as a hard copy. Certain challenges arise as to the admissibility of electronic copies in terms of meeting the requirements of writing, signature, and originality.

Communications from websites or e-mails are not written documents in the traditional sense of letters, hard copies, or physical mail. The existence of an e-mail for instance, may be denied by the originator and where there is no law that provides for the recognition, dispatch, and receipt of data messages, the court may admit the evidence in court but it will have little or no evidential weight. The same rule applies to the admission of computer print-outs as an original copy where several other copies could also be originals.

Some of these challenges have been addressed by the enactment of the Evidence Act which repealed the provisions of the Evidence Act Cap E14 2004 under which the definition of document was restricted to paper records. Before the enactment of the 2011 Evidence Act, the courts battled with the rules in an attempt to deal with computer records whenever they came before them.

81 See *OB Nigeria PLC v OBC Ltd* (2005) 123 LRCN 191.

In Nigeria today, in terms of the provisions of section 84 of the Evidence Act, electronic records are fully admissible in evidence and bear full weight provided all necessary requirements for tendering the documents have been met. The re-enactment of the Evidence Act in Nigeria represents a turnaround in Nigerian legal practice and e-commerce as it broadens the scope of admissible documents to include e-documents. The different requirements for the authentication of a document are considered below.

(a) Writing

Writing is required in contract formation under various circumstances; otherwise the courts would be left with the herculean task of attempting to infer intent and content from the conduct of the parties. Writing and expressions of writing in the Interpretation Act are defined to include printing, lithography, photography, typewriting, and other modes of representing or reproducing words or figures in a visible form.[82]

The Evidence Act recognises data messages and provides for their admissibility. "Document" under the Evidence Act is defined to include:

> Any disc, tape, sound track or other device in which sounds or other data (not being visual images) are embodied so as to be capable (with or without the aid of some other equipment) of being reproduced from it; and any device by means of which information, is recorded, stored or retrievable including computer output.[83]

Sections 51 and 52 of the Evidence Act admit as evidence, electronic records kept regularly in the course of business, or electronic copies of public records that are kept in the exercise of a duty. The Evidence Act further admits into evidence communications produced by a computer under the following conditions.

(a) The communication was produced by a computer during a period in which the computer was in regular use.

(b) The communication was supplied in the ordinary course of business.

82 Interpretation Act LFN 2004 s 18(1).
83 Evidence Act s 258.

(c) At the time of supplying the information, the computer was operating properly.[84]

It is immaterial whether the communication was supplied by human intervention or by automated means. Before the communication becomes admissible, it must, having satisfied the above conditions, be tendered together with a certificate identifying the document which contains the communication. The certificate should give particulars of the device used, the working condition of the device at the material time, and should show that it was made to the best of the knowledge and belief of the party seeking to tender it.[85] The failure of a party to meet the requirements set in section 84(2) of the Evidence Act is fatal, and results in the inadmissibility of the documents sought to be tendered in evidence. In *Dr Imoro Kubor v Hon Seriake Henry Dickson,*[86] the Supreme Court held as worthless exhibit "D" which was tendered by the first respondent (Hon Dickson) on the ground that being an internet print out of the Punch Newspaper, failure to fulfil the conditions precedent to tendering such evidence rendered it inadmissible. The court relied on the provisions of sections 90(1)(c) and 102(b) of the Evidence Act which classified the document as a public document upon which there must be certification.[87] The court held further that if the documents were to be admitted as computer generated records, they still would have been inadmissible as declared by the lower court since the conditions precedent to admitting computer evidence in section 84(1) of the Evidence Act were not fulfilled.[88] What the court has shown here is that e-documents are generally admissible in evidence provided that they are properly tendered in accordance with the procedure in section 84(2) of the Evidence Act.

(b) Signature

Every written document giving rise to a legal obligation is authenticated by means of a signature which binds the maker to accepting responsibility for the contents of the

84 Evidence Act s 84(2).
85 Evidence Act s 84(4).
86 *Dr Imoro Kubor v Hon Seriake Henry Dickson* (2014) 4 NWLR (Part 1345) 534.
87 *Dr Imoro Kubor v Hon Seriake Henry Dickson* Judgement of the Supreme Court SC 369/2012 (unreported) delivered on 25 October 2012, 34-35.
88 Ibid.

document provided other conditions are met – for instance, the additional signature of a witness where the law requires it. The relevance of signatures in documents cannot be underestimated, they create binding consequences, prevent the maker from denying the contents of the document, and give legal force to the content of the document.

According to Atiyah[89]

> The contract is binding because the parties intend to be bound, it is their will or intention … it is their decision and free will which makes the contract binding and determines its interpretation in the event of a breach.

In e-contracts or transactions, the requirement of consent evidenced by an act of the maker is equivalent to a signature. Where it is shown that a recipient or consumer did not give proper consent, the contract will not be enforceable against the consumer. The issue here is that without consent which is premised on the principle of *consensus ad idem* (the meeting of minds), there can be no contract, either conventional or in cyber-space. The question now is in the absence of a regulatory framework for e-transactions in Nigeria, can Nigerians contract online?

Section 93(2) of the Evidence Act provides that "where a rule of evidence requires a signature, or provides for certain consequences if a document is not signed; an electronic signature satisfies that rule of law or avoids those consequences."

The Evidence Act further provides:

> An electronic signature may be proved in any manner, including by showing that a procedure existed by which it is necessary for a person, in order to proceed further with a transaction to have executed a symbol or security procedure for the purpose of verifying that an electronic record is that of the person.[90]

From the provisions of the Interpretation Act,[91] a signature could also be "a mark" especially by a person who cannot write his or her name. As is reflected in the Evidence Act, a click on an "agree", "continue" or "proceed" button satisfies the

89 Atiyah (1978) 94 *LQR* 193.
90 Evidence Act s 93(3).
91 Interpretation Act s 18.

requirement of an e-signature. These provisions are very apt and they reflect the current position on e-signatures.[92] The law provides a technology-neutral environment and recognises assent as a functional equivalence for signature.

(c) Original

Under the Evidence Act the contents of a document may be proved by either primary or secondary evidence.[93] The primary evidence of a document is the document itself, that is, the original. However, in special cases secondary evidence may be admissible. Online, a web agreement that is saved offline satisfies the requirement of an original document, provided it is accessible and can be reproduced for subsequent use.

The requirement for an original document alludes to the integrity of the content of the document to ensure that an agreement is not subsequently altered by one of the parties without the consent of the other party. The confusion surrounding computer print-outs arises from the fact that every copy is an original, and alterations on an electronically signed soft copy do not leave any physical evidence (as do changes to hard copies). This problem is not peculiar to one legal environment and it could be resolved by the use of a portable document format (pdf) and screen shots.

On the issue of determining which copy of a computer print-out is an original – whether it is the very first copy or all subsequent copies – the Evidence Act provides that

> where a number of documents have all been made by one uniform process, as in the case of printing, lithography, photocopy, computer or other electronic or mechanical process, each shall be primary evidence of the contents of the rest: but where they are all copies of a common original, they shall not be primary evidence of the contents of the original.[94]

This implies that every copy printed on the first occasion is an original, but all subsequent print-outs can only be secondary evidence of the document. It is the duty

92 Kazeem *Electronic contract formation* 7.
93 Evidence Act s 85.
94 Evidence Act s 86(4).

of the parties to ensure the preservation of the original electronic agreement or document so that the original can be compared with subsequent or secondary copies.

(d) Evidential weight of electronic records

From the preceding paragraphs, electronic records kept in the course of business, or in public records including all other e-communications, are admissible in evidence with their full weight when tendered in accordance with the provisions of the Evidence Act.[95]

8.2.2 Formalities for electronic contracts

Formal rules on pre-offer, offer, dispatch, receipt, time and place of acceptance, party autonomy, capacity, and incorporation of documents, are accepted rules of contract.[96] The challenge, however, is that their application to the online environment may not always be appropriate. This militates for the adoption of some new rules for online contract formalities in addition to existing rules.[97]

8.2.3. Party autonomy

When contracts are created by parties, they are at liberty to adapt terms to suit their needs. Such terms should, however, be clear and precise so that the courts can adopt them provided that they are not unconscionable.
In *Manya v Idris*[98] the court held as follows:

> Where two free and able parties entered into an agreement the court has a duty to hold them down and give effect to their contract no matter how inelegantly or

95 Evidence Act s 84.
96 Sagay *Nigerian Law of Contract* 6.
97 The basic elements of offer and acceptance in contract formation are discussed in detail in Chapter 2, para 2.6.
98 *Manya v Idris* (2000) FWLR (Pt 23) 1237 at 1250; see also *Ogundepo v Olumesan* (2012) 203 *LRCN* 163.

> ineptly couched. It will be demanding too much of any court to approve unjustified departure from or rewrite such contract except such a contract or part thereof had been properly abrogated.

Parties to a contract are consequently free to bind themselves through agreement on the rules that will apply to jurisdiction, place of contracting, and remedies in the event of breach. Where, however, the parties fail to agree proactively on these terms, the general principles of law will apply as default rules.

8.2.4 Incorporation by reference

The law gives legal effect to acts or documents connected to a particular agreement – whether written or oral when there is evidence of such acts or terms.[99] Similarly, terms incorporated into e-communications through UELAs or URL enjoy validity and could thus be enforced against the parties provided the terms are conspicuously referred to and do not offend the common-law principle of unconscionability. The courts would, therefore, enforce click- or shrink-wrap agreements entered into in accordance with the requirements of the law.

The above postulation, however, is not settled law as each case must stand or fall on its own merits. In *Ogundepo v Olumesan*[100] the court held that where parties have embodied the terms of their relevant agreement(s) in written documents, no extrinsic evidence is admissible to add to, vary, subtract from, or contradict the terms of the written instruments. Generally, there is a legislative *lacuna* in the Nigerian law of contract, in that there is no legislative enactment on terms that could be considered unconscionable. The determination of this is subjective and not easily established, and the courts are not readily persuaded to reconsider terms of a contract to which a party may refer to as extrinsic or incorporated evidence. In *Babatunde v Bank of the North*

---

99 A contract could be formal in which case it must be written and need not furnish consideration while a simple contract need not be written but must furnish consideration, see Sagay *Nigerian Law of Contract* 2-3.

100 *Ogundepo v Olumesan* (2012) 203 LRCN 163.

Ltd & Ors[101] it was held that in the interpretation of contractual transactions, the court will always hold parties bound by the terms of their agreements when construed according to the strict, plain, and common meaning of the words as they stand in the instrument.

In consumer contracts however, reliance on section 129 of the FCCPA could protect consumers from unfair terms. Courts must therefore infer whether terms are fair or not, in terms of the FCCPA.

8.2.5 Legal protection for electronic payment systems

A secured payment system is enabled by strict policies on the privacy of personal financial information. Privacy protection is ensured under the Nigeria Data Protection Regulation 2019[102] and is further enshrined in the Nigerian Constitution. The privacy of citizens, their homes, correspondence, telephone conversations, and telegraphic communications are guaranteed by constitutional provisions.[103] This right to privacy applies to citizens' personal financial information and has been enforced by the courts in a number of cases.[104] The use of e-payment systems, and especially credit or debit cards, is interconnected with online transactions. In Nigeria, payments are made for online transactions through cards, EFT, and more recently, mobile transfers.[105] The non-regulation of the payment system could lead to financial loss for consumers in the event of fraud, stolen cards, invasion of payment information, or mistakes arising from the use of such methods. Although there is no comprehensive legislation on payment security, online financial transactions in Nigeria are regulated by the Central Bank of

101 *Babatunde v Bank of the North Ltd & Ors* (2012) 206 *LRCN* 70.

102 The Nigeria Data Protection Regulation 2019 was developed in accordance with the provisions of the National Information Development Agency Act of 2007.

103 1999 Constitution FRN (amended) s 34.

104 See *Tournier v National Provincial Bank* (1924) 1 KB 461; see also the case of *Anene v Airtel* (unreported) FCT/HC/CV/545/2015 where the court held that sending messages to a subscriber without consent was a violation of his or her right to privacy; similarly, this line of reasoning was followed by the court in *MTN Nig Ltd v Anene* (2018) LPELR 44447 (CA).

105 Use of mobile phones to make payments and transfer funds in Nigeria is very high and soars on increasingly, a fact noted by the CBN in the CBN Guidelines at para 1.4.

Nigeria under the Guidelines on Electronic Banking in Nigeria (CBN Guidelines).[106] The CBN also regulates card issuing schemes.

8.2.5.1 CBN Guidelines on Electronic Banking in Nigeria

The CBN Guidelines protect consumers' financial information through technology and security standards. Based on the Guidelines, banks are required to apply networks that meet specified standards of data confidentiality and integrity before they are used for the transmission of financial data.[107] The Banks' policy on privacy is:

(a) Customer's personal data must be used only for the purpose for which they are compiled.

(b) Consent of the customer must be sought before the data is used.

(c) A data user may request, free of cost, the blocking or rectification of inaccurate data, or enforce a remedy against breach of confidentiality.

(d) Before processing children's data, the consent of the parents must have been obtained and this should be verified by regular mail.[108]

In addition, consumers must be given an option to decline to permit the banks to share "any information about a customer's personal needs, interests, financial position, or banking activity with third party for cross-marketing purposes."[109]

The banks must also implement banking systems in e-transactions that meet the provisions of the technology and security guidelines in the areas of authentication, non-repudiation, authorisation, integrity, and confidentiality.[110] Security requirements include the use of proxy- type firewalls that can prevent a direct connection between

106 The CBN Guidelines was released in August 2003 and has been in effective implementation especially as there is no e-banking legislation in Nigeria despite a clamour for the introduction of e-banking legislation since the setting up of the CBN Guidelines. See para 3(b) of the CBN Guidelines.

107 CBN Guidelines para 1.1.

108 CBN Guidelines para 3(d).

109 CBN Guidelines para 4.1(g).

110 CBN Guidelines para 4.2(d).

the banks back-end systems and the internet, as well as proper physical access controls over all network infrastructures both internal and external. Logical access control should include infrastructures that can detect and prevent password guessing and cracking, and back-door traps in programmes. The control should also be able to detect attempts to overload the system using distributed denial of service (Ddos) and the denial of service (DoS) attacks.[111] Furthermore, the audit trail of all transactions online is a prerequisite for all banks.[112]

8.2.5.2 Card issuing scheme

To minimize the incidence of fraud, cards can only be issued by deposit-taking institutions which must have undergone the rigours of registration with the CBN, while ISPs are to ensure that only websites of CBN's duly licenced financial institutions are hosted on their servers.[113] This provision is very effective in minimising the incidence of fraud because it is actually easier to subject registered entities to the requirements of the law through sanctions, criminal and civil liabilities, as well as seizure of their licences, where applicable. Otherwise, where unregistered card issuers are empowered by online financial platforms, there will be no veil of incorporation to lift in order to detect the anonymous faces behind the websites.

Cards in Nigeria use the chip (smart card) technology rather than the magnetic stripe technology which was in use at the onset of card payments in the country. The CBN Guidelines impose liability on banks for fraud arising from skimming and counterfeiting,[114] except where it can be shown that the merchant was negligent. Moreover, cardholders are not exempted from liability for fraud arising from PIN misuse.[115] Where the customer's negligence has led to fraud or forgery, the bank is

111 CBN Guidelines para 1.5.3.
112 CBN Guidelines para 4.1(d).
113 CBN Guidelines paras 1.4.8-1.4.9.
114 CBN Guidelines paras 1.4.8-1.4.9.
115 CBN Guidelines para 1.4.2(d-e).

entitled to debit the customer's account as a result of the breach.[116] The extent of a bank's liability in respect of the card scheme is unlimited, so that it imposes strict liability even on outsourced products.[117] The CBN Guidelines make the banks responsible for all security measures, notwithstanding that some services may be outsourced to ISPs.[118]

As far as the issue of charges is concerned, charges are not to be deducted from consumer's account without prior authorisation.[119] However, where charges are deducted without authorisation, the consumer must, upon notification, complain within a reasonable time otherwise he or she is presumed to have consented to the charges.[120] Regrettably, stop orders cannot be effectively implemented in the banking system except within specified time frames and subject to prescribed conditions.[121] Paragraph 3 of the CBN Guidelines recommends that strict criminal and pecuniary sanctions are imposed on banks guilty of default by its terms.

8.2.6 Consumer protection and information requirements

The requirement that suppliers of goods and services must provide accurate and non-misleading information to their customers is aimed at ensuring that purchasers are not misled into buying goods or services through misrepresentation and non-disclosure. There are instances where representations made in connection with a sale become an implied part of the terms of the contract. This is based on whether the representation was expressed as a mere opinion, or as a fact upon which the sale was based.[122] Misrepresentation in Nigeria is governed by a mixture of common-law rules and the doctrine of equity. Where it is found that there has been misrepresentation in an

116 See *Bank of the North v Yau* (2001) 5 SC (Part 1) 121, 148-9.

117 The issuing of cards in Nigeria is mostly outsourced in order to save financial resources, focus on the business, expand customer product offerings, and could be due also to lack of necessary technical expertise. See further Olukole *Nigerian Electronic Banking Law* 61.

118 CBN Guidelines para 1.0.

119 CBN Guide to Bank Charges 2004 s 10.

120 *Thor Ltd v FCMB* (2005) 6 SC 9.

121 CBN Guidelines para 3.

122 Sagay *Nigerian Law of Contract* 237.

agreement, or that the sale fails to conform to implied terms, the contract can be rescinded.[123]

Consumers in Nigeria are protected from misrepresentations and are entitled to the benefits of express and implied warranties under the Sale of Goods Laws which have been enacted in different states within the Federation.[124] The Sales of Goods Law as applicable in different states of the country derives its origin from the English Sale of Goods Act, 1893 of the UK.[125] For purposes this study, the Sale of Goods Law of Bendel State of Nigeria, as applicable to Edo State of Nigeria (SGL), will be considered.[126]

8.2.6.1 Consumer protection and implied warranties under the Sale of Goods Law

Consumers enjoy some level of protection under the SGL and these are discussed below.

(a) Condition as to right to sell[127]

In a contract of sale, except as otherwise indicated, in every sale there is an implied condition on the part of the seller that he or she has a right to sell, and this right implies that the consumer has an implied warranty that he or she will have and enjoy quiet possession of the goods. There is also an implied warranty that the goods are free from any charge or encumbrance.

(b) Correspondence with description[128]

The SGL provides that where the contract for the sale of goods is by description, there is an implied condition that the goods and their description will correspond. This provision can also apply to goods sold online where the goods are described pictorially

123 Ibid.
124 Consumer Awareness Organisation *Research report* 101.
125 Sale of Goods Act, 1893 Ch 71 UK repealed by Sale of Goods Act 1979 Ch 54 UK s 63.
126 Laws of Bendel State Cap 150 vol vi.
127 SGL s 13.
128 SGL s 14.

and in writing. And where the sale is by description and sample, the goods must conform to both the descriptions and the sample.

(c) Fitness for purpose and merchantable quality[129]

Generally, the SGL does not provide implied conditions as to quality or fitness for purpose. This implies that at purchase the buyer accepts responsibility for his or her choice. However, there are four exceptions to this general exclusion.

(i) Where the buyer expressly or by implication makes known to the seller the purpose for which the goods are required. This exception can also apply to e-commerce in situations where the goods are personalised or based on specifications.

(ii) Where the goods are bought by description from a seller who deals in goods of that sort, it is immaterial whether or not he or she is the manufacturer, provided that if the buyer has examined the goods, there will be no implied condition as regards defects which the examination ought to have revealed. An online purchaser can take advantage of this exception since he or she has no opportunity to physically examine his or her order.

(iii) An implied warranty or condition as to quality or fitness for a particular purpose based on trade-usage.

(iv) An express warranty or condition that is not inconsistent with the law.

There are interesting provisions in the SGL that could be implemented to benefit an online consumer. The SGL provides in section 29, that unless otherwise agreed, delivery of goods and payment of the price are concurrent conditions – this provision is effective in on-premises sale. On the other hand, in section 35 of the SGL it is provided that:

> Where goods are delivered to the buyer which he has not previously examined he is not deemed to have accepted them unless and until he has a reasonable opportunity of examining them for the purpose of ascertaining whether they are in

129 SGL s 15.

> conformity with the contract. Unless otherwise agreed, when the seller tenders delivery of the goods to the buyer, he is bound on request to afford the buyer a reasonable opportunity of examining the goods for the purpose of ascertaining whether they are in conformity with the contract.

This provision serves as a cooling-off provision in e-commerce contracts and could be so adapted. In fact, one of Nigeria's foremost online stores, Konga, applies this principle and receives payment only after the goods have been inspected by the consumer upon delivery.[130] Furthermore, under the SGL once goods are rejected, the buyer is not bound to return them provided the seller has been informed.[131] The distinction here is that under internationally agreed principles, the consumer is responsible for the cost of returning the goods to the supplier.[132] Unfortunately, in Nigeria, not all online stores accept or exchange returned goods.[133]

Furthermore, in the SGL there is a section that could work against the right of cancellation if improperly applied. Section 38 provides[134] that buyers will be liable (it is presumed that this section will not apply if notice of cancellation is given within a reasonable time) to the seller for any loss occasioned by his or her neglect or refusal to take delivery of goods within a reasonable time after the point at which the seller is ready to deliver the goods. It is arguable that this section is subject to section 35 of the SGL which gives the buyer the right to examine the goods physically before indicating acceptance. E-commerce consumers will, therefore, not be caught by the provisions of this section of the SGL, not having had the opportunity to inspect the goods physically and accept them before the seller is ready to make delivery. Under the SGL the buyer bears the risk of the condition of the goods before delivery in distance sales, unless otherwise agreed.[135] This provision certainly works against the interest of an online

130 Punch "Konga extends pay on delivery to Abuja" 12 February 2019 available at https://punchng.com/konga (date of use: 05 October 2020).
131 SGL s 36.
132 See CRD art 14.
133 See for example, return policy on www.konga.com (date of use: 05 July 2020).
134 SGL s 38.
135 SGL s 34.

consumer as he or she has no means of determining the condition of the goods before they are sent.[136]

In respect of performance, the SGL provides that where goods which have been ordered are not delivered, the buyer can institute an action for damages for non-delivery. This could be the estimated loss resulting directly in the ordinary course of events from the seller's breach of contract. The buyer could also sue for specific performance.[137]

Finally, the expansive provisions of the SGL and the common law on contract provide some basic principles on implied conditions of sale which correspond to description, fitness for purpose; as well as some underlying rules on information which must be provided to consumers in order for suppliers not to fall short of full disclosure. The SGL as it stands, however, does not adequately meet the needs of consumers who do business online. Under the SGL there is a protective measure whereby a sample of the goods on offer could be tendered in evidence to establish their quality against what was actually sold. This advantage is not available to an online consumer whose sample is a downloaded image or a written description of the product. It is also not enough to describe the functions of a digital product without reference to its compatibility to certain operating systems. It is important that consumers are informed of the type of devices on which specific digital products will function properly.

8.2.7 Limitations of conventional rules

The formalities in contractual relations as they apply to offer and acceptance and time and place of contracting, have not been well adapted for application online. There is doubt as to which principles a court will follow in determining the efficacy of an electronic acceptance in that arguments still abound as to whether or not e-

136 See s 20 of the CRD which places the risk on the supplier before delivery.
137 SGL s 52.

communications – especially via e-mail – are instantaneous or third party linked.[138] In the absence of express agreement by the parties, the law is entirely inadequate in determining the location of the parties, and, consequently, the place of an online contract.

It has been concluded that anonymity on the internet cannot be sufficiently cured by reference to the address of a website or an e-mail, nor can the theories of connecting factors help parties in a digital sale or provision of online services.[139] Besides the problem of determining jurisdiction which is closely linked to the location of the parties, the absence of information on the physical address of a supplier would make tracing a supplier who failed to deliver goods or services impossible.[140]

For internet transactions and the sale of digital products, there are specific information requirements that can neither be ignored nor resolved through existing laws.[141] These requirements are peculiar to the online environment without which consumers would be disadvantaged. Consumers must be provided with the opportunity to review and confirm their orders before payment. Taking the simple case of a consumer who transfers ₦50 000 (fifty thousand naira) in place of ₦5000 (five thousand naira) through an e-payment platform; the error lies in the insertion of an additional digit and this translates into a loss, and considerable worry and strain in retrieving the extra amount from the merchant. This form of error is unlikely in the case of physical payments. There must also be rules guiding information on cancellation and refunds, without which retrieving an overpaid sum or returning non-conforming or damaged goods may not be an easy matter for the e-commerce consumer.

Another area of concern is that as there are no specific obligations on website owners who provide services to consumers, other than to apply the supplier's personal codes. Nigerian consumers will therefore, be at a considerable disadvantage compared with

138 Snail (2008) 2 *JILT* 8.
139 Tang *Electronic Consumer Contracts* 14.
140 Ibid.
141 Pistorius (2002) 35 *CILSA* 129.

their counterparts from other countries who enjoy a series of rights, including the right of withdrawal and cancellation; right to refund, information, protection from direct commercial communications, and inertia selling.[142] Although the right to cancel is provided in section 120 of the FCCPA, the right is limited to the cancellation of reservations or advance orders. For online transactions, there is the need for the expansion of the right to cancel or withdraw beyond reserved or advance orders. The right to cancel or withdraw from a transaction should be available to consumers within a reasonable period of time after payment. This reasonable period of time is aptly referred to as the window period in other jurisdictions.

The principal document governing payment systems is the CBN Guidelines, which have provided substantial privacy rules for online payment information. However, they appear to have neglected consumer protection measures in terms of information both before and after debiting a cardholder, and procedures for refund of payments improperly made. Sanctions in respect of unauthorised debits, overpayments, debits for unordered or undelivered goods or services, and overcharging, are not covered in the CBN Guidelines. This inadequacy needs to be addressed for an effective card and online payment system in Nigeria. Fundamentally, there are no redress systems that are appropriate to the online environment in terms of ADR. These should include an online dispute resolution system or a cyber-court. Without an online or appropriate redress platform, a Nigerian consumer resident in State A who buys a product from an online retailer in State B, may not find travelling to State B to litigate on a ₦5 000 (five thousand naira) dispute viable, where the cost of hiring counsel, travel, and hotel accommodation may well exceed ₦50 000 (fifty thousand naira) – not to mention the time, inconvenience, and delay involved in the process.

The CBN Guidelines, the Cybercrimes (Prohibition, Prevention, etc) Act and most especially the FCCPA on one hand offer different levels of protection for e-commerce consumers but nevertheless these legal instruments are unable to prohibit unfair

142 For instance, these range of rights are provided for in the CRD.

practices against consumers in the form of: unfair contract terms, misleading advertisements, cancellation, delivery, refund policies and dispute resolution. The E-transactions Bill on the other hand is drafted specifically to address the needs of e-commerce consumers and is able to resolve most of the challenges faced by e-commerce consumers. The provisions of this Bill are considered in what follows.

8.3 Electronic Transactions Bill 2017

The E-transactions Bill is a Bill for an Act to facilitate the use of information for conducting transactions in electronic form in Nigeria.[143] The Bill provides for e-transactions and data protection. It seeks to provide a legal and regulatory framework for conducting transactions using electronic or related media, and the protection of the rights of consumers and other parties engaging in e-transactions and services, and seeks to facilitate e-commerce in Nigeria.[144]

8.3.1 Provisions of the Bill

The Bill applies to the use of information in the form of electronic or other media. It applies to both business and consumer contracts. The use of "documents" in the Bill applies to all forms of data. The definition of a document as contained in the E-transactions Bill is that

> document includes a representation of information in precise, formalised language in or on a medium from which it can be read, or from which it can be retrieved in a form in which it can be read or perceived, a representation of data on or in a data medium from which it is retrievable, such that it is readable in or on the medium, or on its retrieval.[145]

The need to understand the definition of a document in terms of the Bill is based on the consistent use of the term "documents" where expressions such as "data" or "data

143 E-transactions Bill, long title.
144 E-transactions Bill Explanatory Memorandum, see also s 1.
145 E-transactions Bill s 45.

messages" could have been used. The direct use of "document" in place of other terms specifying electronic input appears to have eliminated the need for functional equivalence in the Bill, and to have translated data, electronic records or media into the regular parlance of "documents."

The provisions of the Bill override the provisions of the Nigerian Communications Act in respect of the transmission of documents as defined in the Bill.[146]

The Bill deals with the validity and evidential value of data messages by integrating the elements of data into "documents." The Bill also makes provision for legal formalities in electronic contracting and covers areas such as: the attribution of documents; the acknowledgement of documents; and rules on dispatch and receipt, time of receipt, and location of parties. Consumer protection, jurisdiction, commercial communications, information requirements, performance, and the limitation of the liability of ISPs are all addressed.

8.3.1.1 Validity of electronic records

Where the use of a document is required by law, that requirement is satisfied if the document is presented electronically as prescribed in the Bill. Information shall not be denied legal effect, validity, or enforceability solely on the basis of the medium or technology by which it is represented or communicated, or because it derives its validity and enforceability by reference to information in some other document.[147] This provision is modelled on the UNCITRAL Model Law and recognises information which is linked or referred to in documents thus recognising UELAs and terms attached to the use of electronic products and services.

(a) Writing

146 E-transactions Bill s 2(5).
147 E-transactions Bill s 3(1).

Section 5 of the E-transactions Bill provides that electronic records or documents fulfil the obligation of writing as required under any law, provided they are accessible and available for subsequent reference. E-documents will however, not be acceptable where the requirement of writing is in respect of the following:

(i) notice of the cancellation or termination of utilities;

(ii) the default, acceleration, possession, foreclosure, or eviction, or a right secured under a credit or a rental agreement, for the primary residence of an individual;

(iii) the cancellation or termination of health insurance or benefits, or life insurance benefits, excluding annuities;

(iv) recall of a product, or material failure of a product, that risks endangering health or safety;

(v) a public notice on any document required to accompany any transportation or handling of hazardous materials, pesticides, or other toxic or dangerous material;

(vi) a public notice to override any statutory provision intended for the protection of consumers.[148]

The limitations on writing by electronic means are expansive and virtually eliminate its use in fulfilling the requirement of writing. These restrictions are connected to the level of illiteracy and digital divide in the country which is exuberated by poor infrastructural development prominent among which, is consistent power failure. Furthermore, regular internet access is not available to a vast section of the population of the country conceding that the majority have access to one form of electronic device or the other.

Given the social, cultural, and economic background of the country, although the limitations appear excessive, they are practical. It would be unimaginable if notices of life-threatening situations are sent electronically to a population who, on average, have access to the internet for only a few hours of a day (basically to access their e-mails and connect briefly to the social media). While this is a situation peculiar to developing economies, the restrictions should not have been total but modified and conditional. Consider the example of notice for the provision or cancellation of utilities, or of health

148 E-transactions Bill s 4(3).

insurance, these are quasi-private communications that can be sent electronically provided prior consent to the use of electronic notification has been obtained from the consumer.

In summary, the term “document” (electronic records) in the E-transactions Bill, applies to the following:

(a) Filing of forms, applications, or any other document with any office, authority, agency or body corporate.[149]

(b) The issuing or granting of any licence, permit, or approval.[150]

(c) Receipt or payment of money in a particular manner.[151]

(d) Publication of information in a Gazette.[152]

(e) Retention of records.[153]

From the above, e-documents can be used as evidence of payments, the grant of licences, the filing of forms, gazetting government information and for the retention of records under the E-transactions Bill.

(b) Signature

The E-transactions Bill does not require a specified format for an e-signature, any method which is used to identify the maker under reliable circumstances and with the consent of the recipient, satisfies the requirement of an e-signature.[154] In *Specht v Netscape*,[155] Judge Hellerstein stated:

> Assent may be registered by a signature, a handshake, or a click of a computer mouse transmitted across the invisible ether of the internet. Formality is not a requisite; any

149 E-transactions Bill s 8(a).
150 E-transactions Bill s 8(b).
151 E-transactions Bill s 8(c).
152 E-transactions Bill s 9.
153 E-transactions Bill s 10.
154 E-transactions Bill s 11.
155 *Specht v Netscape* 306 F 3d 17 - Court of Appeals 2nd Circuit 2002.

> sign, symbol or action, or even willful inaction, as long as it is unequivocally referable to the promise, may create a contract.

Where, however, a particular law, or recipient of the communication, specifies a particular format, only that format will satisfy the requirement of an e-signature.[156] The twist in the E-transactions Bill, however, is the condition that e-signatures created outside of Nigeria, must satisfy the Nigerian Certification Standards in accordance with the rules prescribed by the NITDA.[157] This latter provision contradicts the freedom of parties to use any method or mark which identifies them and shows their intent, without the necessity of subjecting such marks or methods to a certification authority.

8.3.1.2 Admissibility and evidential weight of electronic records

In accordance with the Bill, a document shall not be denied admissibility solely on the ground that it can neither be confirmed nor denied owing to the medium or technology used.[158] The weight to be attached to documents where they are admitted in evidence is determined by the following:

(a) reliability of the manner in which the information was generated, stored or communicated;
(b) reliability of the manner in which the integrity of the information was maintained;
(c) the manner in which its originator was identified; and
(d) any other relevant factor.

The determination of evidential weight in documents as provided in this section does not apply to the practice and procedure of a court or tribunal.

156 E-transactions Bill s 11.
157 E-transactions Bill ss 13-14.
158 E-transactions Bill s 3(1), see also s 84 Evidence Act.

8.3.1.3 Electronic contracts

Contracts conducted electronically either in person or by e-agents are recognised and valid under the Bill.[159] Contracts between a person and an e-agent will only be valid if they satisfy the following two conditions:

(a) the party who is a natural person knows or has reason to know that he or she is dealing with an e-agent; and

(b) the natural person believes that the transaction will be performed through the action of the e-agent.

The import is that where a party transacts with an e-agent unknowingly, he or she may, upon becoming aware of that fact, rescind the contract.

The Bill recognises the exchange of offer and acceptance electronically,[160] but limits the electronic use of offer and acceptance in certain transactions to be determined by the NITDA or any appropriate regulatory body.[161]

8.3.1.4 Attribution

One major concern in e-transactions lies in giving evidence as to the source of a document. Electronic addresses can be deceptive – for example, in the case of identity theft a user could create a similar website and design, and pass it off as the original website; or a user could create an e-mail account with a very similar name to that of another so that a cursory look could mislead a recipient or addressee. In order to achieve certainty, rules on attribution of documents online are essential. In the Bill, documents are attributed to the originator if they are sent directly, or by someone with authority to do so, or by an information system programmed by or on behalf of the

159 E-transactions Bill s 26.
160 Ibid.
161 E-transactions Bill s 26(6).

originator, to operate automatically.[162] This provision will not apply if the addressee receives a notice from the originator repudiating the source of the document, provided the notice is given within a reasonable time.

8.3.1.5 Dispatch and receipt

The rules governing dispatch under the E-transactions Bill are a replication of the provisions in the UNCITRAL Model Law. However, the application of this section is restrictive; the Bill provides that the NITDA or any appropriate regulatory body may by regulation, restrict the application of the rules governing dispatch and receipt in respect of "certain communications."[163] These communications are, however, not specified in the Bill or in the NITDA Act.

8.3.1.6 Delivery and acknowledgement

Where documents are delivered electronically, the originator may require that receipt of the document is acknowledged by the addressee. The acknowledgement may be requested in a particular form, and where that is the case, there is a presumption that only an acknowledgement in that form will be recognised.[164] In all other cases where there is no specified format for an acknowledgement, any communication by the addressee, whether automated or otherwise, or any overt conduct of the addressee, will be deemed a proper acknowledgement.

In addition to requesting an acknowledgement, the originator may further state that the delivery of the document is subject to receipt of an acknowledgement. In such a case, unless an acknowledgement is received, there is an assumption that there has been no delivery. Where, however, the originator has requested an acknowledgement but has not stated that the delivery of a document is conditional on receipt of that

162 E-transactions Bill s 27.
163 E-transactions Bill s 29(6).
164 The presumption is due to the fact that the law is silent on the point.

acknowledgement, and the acknowledgement has not been received by the originator within the time specified or agreed, or, if no time has been specified or agreed, within a reasonable time, the originator may be required to give notice to the addressee informing him or her that no acknowledgement has been received. At that point the originator may specify some other reasonable time, and if the acknowledgement is not received by that time, the originator may, upon notice to the addressee, treat the document as though it had never been sent.[165]

It should be noted that under the Bill there is no presumption of law that the document received in an electronic message corresponds to the document sent.[166] This provision contradicts section 153(2) of the Evidence Act which provides:

> The court may presume that an electronic message forwarded by the originator through an electronic mail server to the addressee to whom the message purports to be addressed corresponds with the message as fed into his computer for transmission…

In construing the effect of both provisions – notwithstanding that the thinking in the Bill is in line with international documents on e-commerce,[167] it is submitted that section 153(2) of the Evidence Act is more appropriate in legal jurisprudence. Suffice it to say that where it is established that a document which has been dispatched has been received, there should be a presumption in law, that the content of the received document corresponds to the content sent. The onus, therefore, should be on the addressee to rebut that presumption by leading evidence to show that the contents differ. In analysing the Bill further, it is clear that the rules on the time and place of dispatch of information are on all fours with article 15 of the UNCITRAL Model Law. The Bill also allows party autonomy.[168]

165 E-transactions Bill s 28, this provision reflects art 14 of the UNCITRAL Model Law.
166 E-transactions Bill s 28(6).
167 See art 14(5) UNCITRAL Model Law.
168 E-transactions Bill s 5.

8.3.1.7 Consumer protection

Sections 32-35 of Part VII of the Bill address consumer issues and proffer safeguards for consumer protection in line with established consumer-protection principles specifically applicable to the online environment. They are principles governing: information requirements; confirmation; protection of personal data; performance; commercial communications and inertia selling; discharge from cost in respect of unsolicited goods; and protection from misrepresentation and non-disclosure.

(a) Information requirements

The information requirements for the goods are fairly comprehensive in terms of existing requirements in the legislative texts of other countries. They do not, however, take cognisance of modern technologies in consumer transactions, or of the use of single-window facilities. Nonetheless, the information which service providers are required to provide in terms of the Bill must be sufficient to enable a consumer to make informed decisions, and should be capable of being saved or printed out. The information must be conspicuously displayed in a language the consumer understands, before the transaction is confirmed.[169]

The Bill provides that a service provider or vendor shall ensure that its marketing practices and information are current and accurate, and are not deceptive and misleading. Where the service provider is in breach of the above information requirements, and there is non-disclosure of a material fact or misrepresentation about the goods which are delivered, the vendor shall not be entitled to claim any charges.[170] Information which is to be provided by the business requires the business to identify itself. The Bill does not specify the mode of identification, and fails to specify that contact details – such as addresses, e-mails, or phone numbers – must be displayed.

169 E-transactions Bill s 32.
170 E-transactions Bill s 33(4).

There is, however, other information on business policies, enquiry, complaint and claim procedures, warranty, and support services which must be provided.

(b) Confirmation and cancellation

Consumer protection will be ineffective in the absence of a process by which consumers are not held to ransom because of input errors. This can be achieved through a review and confirmation process, and the opportunity to withdraw or cancel a transaction within specified time limits, otherwise known as a window or cooling-off period.

This protective measure is captured in section 33 which provides that a consumer shall first be alerted to the terms in a contract, and secondly, shall be provided with an option to correct or cancel the order *before* it is accepted or processed. It should be noted that failure to provide a consumer with an opportunity to review or cancel, discharges the consumer from any obligation to pay charges.[171] The loophole in this provision, however, is that the protection is extinguished after the order has been confirmed. There is, therefore, no window or cooling-off period for consumers to cancel or withdraw from online contracts after confirmation as permitted in the EU.[172] The only opportunity to cancel after confirmation is in relation to on-going contracts, during which period there is material change in the goods or services. When this happens, the consumer must be given the option to decline further supply of the goods and services through a simple and cost-free method of cancellation.[173]

(c) Commercial communications and inertia selling

E-transactions expose the consumer to invasion of his or her personal data, identity theft, and hacking. With the help of cookies and other tools, personal information are gathered and used for unsolicited electronic mailing. Under the E-transactions Bill

171 E-transactions Bill s 33.

172 Compare with art 9 of the CRD which permits withdrawal after purchase within fourteen days and further provides for re-imbursement in art 13, where the consumer has already made payment before withdrawing from the transaction.

173 E-transactions Bill s 33.

unsolicited communications are permitted provided they include a prominent display of the source of the communication, and a return address. The communication must also provide a simple procedure by which consumers can notify the sender of their intention not to receive further messages, that is, there must be an opt-out option. Although the procedure for opting out should be simple, the Bill fails to provide that opting out should be at no cost. This is trite otherwise the imposition of charges may discourage consumers from exploring the option of opting out.[174]

In terms of the Bill, consumers are not liable to payment of charges for unauthorised transactions, and that would include unsolicited goods. Therefore, inertia selling, although not expressly prohibited through the imposition of civil or criminal penalties under the Bill; is not sanctioned and cannot form the basis for an action to claim or enforce payment.[175] The consumer is under no obligation to pay for unsolicited goods or services, even after consuming them. Furthermore, lack of response to such offers or services does not imply consent.

(d) Performance

Performance in a contract is highly circumspect and may be enforced in various ways against the party in breach. While there are clear provisions advising caution as regards performance within reasonable time, the E-transactions Bill does not provide a time limit within which performance must be carried out before the consumer may cancel the contract. However, section 33(2) of the Bill empowers consumers to cancel their orders when the suppliers fail to fulfill their obligation within stipulated or reasonable time frames.

(e) Privacy

The confidentiality of the consumers' information is guaranteed under the Bill. Privacy policies are to be made public and should be easily accessible to the consumer before

174 E-transactions Bill s 35.
175 E-transactions Bill s 33(4a).

the commencement of any transaction.[176] Consumers must be informed through privacy policies on the use and disclosure of their personal information, how they may give and withdraw consent on the use of their personal information, and the implications of such choices. Consumers should also be informed as to how they may review, correct, or remove such information. On sites where cookies are used, consumers should be informed on how and why they are used, and the consequences of a consumer's refusal to accept a computer cookie. A service provider is not permitted to collect, use, or disclose a consumer's personal information inappropriately or to disseminate the information without the prior consent of the consumer. Vendors or service providers may not, as a condition for a transaction, require a consumer to consent to the collection, use, or disclosure of personal information beyond what is necessary to complete the transaction.[177]

Finally, the responsibility of vendors to protect the personal information of their customers extends to third parties. Before the transfer of information, the vendor is required to ensure, by contractual or other means, that the third party complies with the privacy provisions of the E-transactions Bill.

8.3.1.8 Limited liability of service providers

It is important for consumers to understand the nature of liabilities surrounding C2B transactions as this will inform the level of reliance which they place on information on websites. In terms of the E-transactions Bill, a service provider or vendor is not liable for providing access to, or providing facilities for transmitting, routing, or storing electronic records, provided he or she does not initiate the transmission; select the addressee; and does not select or modify the electronic record. The storage of electronic records does not attract any liability relating to damages arising from the

176 E-transactions Bill s 34(2).
182 E-transactions Bill s 34(4).
177 E-transactions Bill s 34(4).

record, unless the service provider is informed or aware of infringing activities on the site.[178]

However, a service provider will not be exempted from liability arising from storage if it has not designated an agent to receive notifications of infringement. It must also inform the public through its services and webpage, of the name, address, phone number, and e-mail address of the agent. A service provider is not expected to bear liabilities arising from damages incurred by a third party through activities involving linking, managing a directory, or using information-location tools.[179] In the Bill, service providers can act upon notifications for take-down without a court order or an order from a monitoring agency. While this may lead to an abuse of the process, and a means of taking undue advantage of third parties, the law provides a deterrent by criminalising the act of generating false notifications. The Bill provides a well thought out procedure for take-down notices. Such a notice must be in writing and should include the full details of the complainant and of the infringement complained of. This section closely follows the take-down notice procedure in the South African ECTA, and similarly, protects service providers from liability arising from a take-down action.[180] Finally, service providers are under no obligation to monitor the activities of third parties on their websites.

8.3.1.9 Dispute resolution

Provision is made for dispute resolution under subsidiary regulations in Part IX of the Bill. Tasks under this part of the law are delegated to regulatory bodies, one of which is the NITDA. These bodies are tasked with establishing standards for service providers or vendors conducting business in Nigeria, in respect of procedures for dealing with complaints; procedures for dispute resolution; the form and amount of compensation

178 E-transactions Bill s 38.
179 E-transactions Bill s 40.
180 Ibid.

payable by service providers and vendors in the event of default in service delivery; amongst other standards.[181]

8.3.1.10 Jurisdiction

The provision of the E-transactions Bill in reference to jurisdiction is well articulated. It resolves the problem of internet jurisdiction in e-transactions in the same way that jurisdictional issues are resolved in the US and the EU. The Bill provide as follows:

(a) In transnational contracts, disputes shall be resolved in accordance with the rules designated by the parties which shall be the substantive law of the country and not its conflict of laws rules, or
(b) Where no rules are designated, the court or arbitral tribunal shall apply the rules of law which it considers most appropriate.[182]

However, in the absence of an agreement, by way of default, where the defendant directs its activities to Nigeria, or runs a branch, agency or other establishment in the country, such a contract shall be subject to Nigerian law.[183] The business does not need to be domiciled in Nigeria. In considering the most appropriate law, regard shall be had to where the supplier directs his or her business activities or has a branch, agency, or other establishment.

8.3.1.11 Electronic payments

The E-transactions Bill recognises e-payments subject to CBN rules and regulations.[184] There is, however, no direct regulation of contractual obligations between financial issuers and consumers. It has been observed from preceding paragraphs that the protective measures in the CBN Guidelines on Electronic Banking are not sufficiently comprehensive to safeguard the interest of consumers in Nigeria.

181 E-transactions Bill s 42.
182 E-transactions Bill s 30.
183 E-transactions Bill s 30(4).
184 E-transactions Bill s 26(5).

Some e-commerce transactions in Nigeria follow the model of payment after delivery due to mistrust and poor protective measures in the event of fraud.[185]
In terms of the E-transactions Bill[186] consumers are, however, protected from charges in the following circumstances:

(a) where the transaction was not authorised by the consumer;

(b) the goods were not delivered within an agreed time;

(c) the goods delivered differed materially from the description provided;

(d) the service provider or vendor failed to provide material information that could affect a decision regarding the goods or services;

(e) there was no option for the consumer to cancel the transaction while acting in good faith.

8.3.1.12 Exclusions

The Bill does not apply to: the creation of a will, or to execution of negotiable instruments, the creation, performance, or enforcement of an indenture, declaration of trust, or power of attorney, with the exception of constructive and resulting trusts. The Bill also finds no application to: a contract for the sale or disposition of immovable property, or any interest in such property; the conveyance or transfer of interest in immovable property; or to documents of title for movable and immovable property. In other words, the use of electronic media will not be recognised in the creation of any document of title.[187]

Discussing the E-transactions Bill has thrown a lot of responsibilities at the doorstep of NITDA, it is proper to submit that the enforcement of most e-commerce consumer rights in Nigeria depends largely on the role of NITDA. NITDA achieves this through

185 Ibam, Boyinbode and Afolabi (2017) *EAI Endorsed Transactions on Serious Games* 4/15 2.
186 E-transactions Bill s 34(4).
187 Such as transferable records.

regulations and guidelines which they are empowered by law to issue.[188] Some of the various regulations and guidelines issued by NITDA are listed below.

8.4 National Information Technology Development Agency Act 2007

NITDA was established in 2007 pursuant to the approval of the National Information Technology Policy.[189] The NITDA is an agency of the Federal Government responsible for the regulation and development of information technology in Nigeria. It achieves its mandate through the development of standards, guidelines and regulations which it issues in accordance with the provisions of section 6 of the NITDA Act. A breach of the guidelines is a punishable offence under sections 17 and 18. So far these are some of the guidelines issued by NITDA[190]:

(a) Guidelines for Registration of ICT Service Providers/Contractors for Delivery of IT Services to MDAs 2018.

(b) Framework and Guidelines for the Use of Social Media Platforms in Public Institutions 2019.

(c) National Information Systems and Network Security Standards and Guidelines 2013.

(d) Guidelines for Clearance of Information Technology (IT) Projects by Public Institutions 2018.

(e) NITDA Public Key Infrastructure Regulations 2014.

(f) Guidelines for Nigeria Content Development in Information and Communications Technology (ICT) 2013.

(g) Data Interoperability Standards 2016.

188 NITDA s 6.

189 NITDA "Background" the National information policy was approved by the Federal Executive Council in April 2001 and the approval led to the establishment of NITDA available at http://nitda.gov.ng (date of use: 15 October 2020).

190 NITDA "Standards & Guidelines" available at https://www.nitda.gov.ng (date of use: 10 October 2020).

(h) Data Protection Regulations 2019.

The NITDA guidelines provide almost exclusively for Government Ministries, Departments, and Agencies (MDAs) with little impact on the private sector. The guidelines do not make up for loopholes in the E-transactions Bill, neither have they provided for those unresolved issues generated in the Bill for the resolution of NITDA.

8.5 Summary and limitations

Reflecting on the E-transactions Bill evidences the adoption of current thinking in certain sections, for instance, the sections dealing with the liabilities of service providers, the acknowledgment procedure in e-communications and jurisdiction are very relevant to current approaches in e-communications. In summary, the use of an electronic form for any communication in Nigeria is not a mandatory requirement of the Bill therefore individuals are precluded from insisting on the use of electronic media in any communication.[191] Within the national context, the Bill can be said to be technology-neutral as it does not mandate technological steps for the authentication of e-signatures, writing, or originality. However, the requirement of section 14 of the E-transactions Bill, that the use of e-signatures created from outside the country would be subject to regulations by NITDA opens up discussions on the neutrality of the technology that is applied.[192]

Still on the E-transactions Bill, it validates the use of electronic media for contract formation, and the rules apply only in respect of formalities, and do not affect the substantive rules governing contract formation.[193]

Section 29(6) of the Bill, however, needs to be addressed in reference to presumption of corresponding documents between an originator and the addressee. The Bill

191 E-transactions Bill s 10(4).
192 For further discussion on this see the NITDA Public Key Infrastructure (PKI) Regulations 2014.
193 E-transactions Bill s 27 (6).

provides that there is no presumption that a document sent corresponds to the document received. This provision in the Bill is contradicted by section 153(2) of the Evidence Act, and this needs to be resolved. It is, however, clear that this provision in the Bill indeed reflects international principles on e-transactions.[194]

In section 33, the Bill conspicuously omits to resolve the problem of anonymity on the internet by failing to specify that businesses should identify themselves by means of contact details such as a physical address, company name, registration number (where registered with the Nigerian Corporate Affairs Commission), and other contact details.

The Bill falls short of internationally-agreed protective measures in terms of its review and cancellation principles. Whereas, e-commerce consumers may withdraw from a contract without reason within an agreed period before and after performance, the Bill limits the protection of consumers against uninformed purchases only before confirmation. This limitation intrudes on the right of consumers to return purchases. Finally, there is no protection for consumers as regards m-commerce and transferable records.

8.6 Conclusion

The concern in this chapter has been in examining the level of protection available to online users in the absence of e-commerce-specific legislation in Nigeria. Flowing from the current state of Nigerian law, consumer protection for online transactions in Nigeria is like an illusion[195] until there is specific legislation governing e-transactions and e-commerce consumer protection. The E-transactions Bill has passed the required num-

194 See UNCITRAL Model Law art 14(5).

195 See Kazeem *Electronic contract formation* 8; see also Ibam, Boyinbode and Afolabi (2017) *EAI Endorsed Transactions on Serious Games* 4/15 2; Ewelukwa (2011) 13 *European Journal of Law Reform* 565.

ber of legislative readings[196] but is yet to receive presidential assent and this makes it inapplicable. The Bill provides for e-commerce and data protection and would have been a first in the history of Nigeria. It's fairly elaborate provisions would no doubt provide additional protection for consumers who do business online.

Various laws embodying direct and indirect measures of protection for e-commerce consumers have been examined and the outcome has been that, due to the peculiarity of the online environment, it is impracticable to protect the legal needs of consumers online by relying on laws which were drafted without an awareness of e-commerce and its characteristics. In comparing the breath of the provisions of a single piece of proposed legislation on e-commerce, which is the E-transactions Bill, to the provisions of every other piece of legislation in the country, it is safe to conclude that e-commerce consumers can only enjoy protection on par with conventional consumers through the adoption of specific laws for e-commerce and e-commerce consumer protection.

196 Placng "E-transactions Bill passes third reading" 18 May 2017 available at http://placng.org (date of use: 25 October 2020).

CHAPTER NINE

CONCLUSION AND RECOMMENDATIONS

9.1 Introduction

The electronic age is no longer merely a novel phenomenon – it is now part of our daily lives. With the internet, there is no final destination but rather continuing technological development. From Chapters Three to Six different rules on the protection of e-commerce consumers within the ambit of e-commerce and consumer protection laws were studied. In Chapter Seven a comparative look at these laws was undertaken and in Chapter Eight there was a review of pieces of legislation relating to consumer protection in a jurisdiction where there is no specific e-commerce and e-commerce consumer protection legislation. In the course of this study, three findings have predominated:

9.1.1 Electronic transaction-specific legislation is required

The application of the common law or legislation in the absence of e-transaction-specific legislation has proved a myth. Drawing from the conclusion in Chapter 8, the application of the FCCPA; Sale of Goods Law; the Evidence Act; and other related legislation notwithstanding, consumers in Nigeria are not adequately protected from the problems associated with e-transactions.

9.1.2 Existing frameworks for online consumer protection are inadequate

In Chapters 3-7 of this thesis, e-transaction-specific legislation at the international, regional, and national levels were examined. After analysing these texts, certain principles common to all the texts, emerged. The regional and geographic spread of these texts notwithstanding, it is clear that no single legislative text or document has adequately provided for consumer protection; and that a mere combination of the

principles in existing texts cannot offer the protection required. This is particularly true of the recent text of the AU Convention which ought to capture basic issues facing technological development. Although there is a great level of protection in the CRD however, some of the issues captured are not adequately addressed. For instance, the CRD has introduced additional information requirements with respect to the use of mobile devices, but has not dealt with ancillary consumer-protection measures which are intrinsic to the use of mobile devices – for example, additional confirmation processes, or requiring network vendors or providers to bear liability in the absence of implementing regulatory codes in order to minimize fraud. The Nigerian E-transactions Bill, 2017, too, does not benefit adequately from recent developments in e-transactions. In a sentence, a large percentage of the existing framework for e-consumer protection across the globe is either obsolete or inadequate.

9.1.3 The need for harmonisation of e-transaction laws

Working through the concerted efforts of different international and regional organisations, as well as the national laws of certain countries, it becomes clear that the harmonisation of e-transaction laws is quintessential to the implementation of consumer protection of those who transact online. While certain principles reverberate through all the legislative texts, they are not couched to provide the same level of protection; this results in differing standards.

Again, the question of cross-border jurisdiction has remained unresolved as internet jurisdiction cuts across all frontiers and no single country can legislate for other countries. Jurisdiction in online transactions can only be said to have been clarified at the level of the EU which has specifically conferred on the consumer, the choice of applicable law and jurisdiction in a consumer contract. There is no international consensus on what rules should apply in determining jurisdiction in e-consumer contracts. Efforts to formulate law on international jurisdiction are still underway under the Hague Convention, and its success will go a long way to, first, ameliorate the plight

of solicitors who have to study as many national laws as possible; and secondly, provide consumers with the much desired certainty in e-transactions.

Finally, the need for a Convention on e-transactions has been reiterated in this study, and it is canvassed that such a Convention will be the most appropriate answer as it will embody all the recognised consumer-protection principles and incorporate emerging principles so as to provide a comprehensive and effective body of law for consumer protection across the globe.

9.2 Conclusions from evaluated instruments

9.2.1 Established consumer-protection principles

From the international and regional legislative texts and documents which were studied in this work, the following principles were generally established and they should be used as a minimum standard for measuring consumer protection across the globe. It goes without saying that not all national laws contain all of these principles. The principles do, however, represent the minimum standard that could be deduced from a holistic reading of all the relevant legislative texts and instruments.

- Data messages and e-communications are valid and meet the requirements of writing.[1]
- A mark or act which signifies consent meets the requirements for an e-signature, and satisfies the requirement of a signature wherever a signature is required.[2]

---

1 This conclusion is drawn from the discussions in Chapter 3 para 3.3.2.2; Chapter 4 para 4.3.1.1; and paras 5.2.1; 5.3.2.1; 5.3.4.1; 5.5.1.1 of Chapter 5. See also the provisions of the texts that were studied in these paragraphs, UNCITRAL Model Law art 5; E-commerce Directive art 9; AU convention art 6; SADC Model Law ss 4 & 6; EAC Framework Phase 1, r 5; and the ECOWAS E-transactions Act art 25.

2 See Chapter 3 para 3.3.2.2; Chapter 4 para 4.3.1.1; Chapter 5 paras 5.2.1; 5.3.2.1; 5.3.4.1 and 5.5.1.1. see further, UNCITRAL Model Law on Electronic Signatures art 6; E-signature Directive recital 16; AU Convention art 7; SADC Model Law s 7; EAC Framework Phase 1 r 5; and the ECOWAS E-transactions Act art 37.

- E-transaction principles do not apply in respect of the alienation of immovable properties, wills and codicils[3], employment contracts[4], taxation, cartel law, legal representation of a client in court, the relationship between a medical practitioner and his or her patient, especially as regards the physical examination of a patient. The same holds true for gambling activities involving wagering stakes.[5]

- E-documents are admissible in evidence and, as with documents generally, other factors will be considered when attaching weight to the evidence.[6]

- Contracts can be formed by means of data communication.[7]

- Contracts formed through the use of e-agents are enforceable, provided that where a contract is formed between a natural person and an e-agent, the natural person is given an opportunity to review and confirm the transaction.[8]

---

3 The exclusion of immovable property from e-transaction regulations is not a generally applied principle. For instance, in Africa, the African Union Convention and the ECOWAS Supplementary Act did not exclude immovable property from the scope of their legislation, while the Common Market for Eastern and Southern Africa Model Law and the East African Community Framework for Cyber-laws Phase 1, leaves the discretion to exclude certain areas to member states. The UNCITRAL Model Law also leaves the right to exclude appropriate transactions from the scope of e-commerce to member states, while EU too, has not excluded immovable properties from the coverage of its community laws on e-transactions. At present the US ULC has passed a law which allows electronic wills known as the Uniform Electronic Wills Act 2019.

4 Employment contracts are generally excluded from consumer protection related laws, this however, does not touch on the validity of a contract or other employment issues that were communicated through data see the case of *Sihlali v South African Broadcasting Corporation Ltd* which was referred to in Chapter 5 para 5.7.3.1(b).

5 For a detailed discussion on items which are excluded from e-commerce laws see Chapter 4 para 4.3.1.2, and the E-commerce Directive arts 1 & 9; para 4.3.2.2 and the CRD art 3; see further Chapter 5 para 5.2.1.1 and the AU Convention arts 2 & 6; para 5.3.2.2 with reference to the SADC Model Law ss 6-7; para 5.3.4.2, and the EAC Framework Phase 1 r 2; para 5.4.1.1, and the COMESA Model Law art 22; and para 5.5.1.1, with reference to the ECOWAS E-transactions Act arts 3 & 26.

6 See Chapter 3 para 3.3.2.2; Chapter 5 paras 5.2.1; 5.3.2.1; and 5.5.1.1. See further, UNCITRAL Model Law art 9; AU Convention art 7; SADC Model Law ss 10 & 20; and the ECOWAS E-transactions Act art 32.

7 On the formation of contract by electronic means see Chapter 3 para 3.3.2.3; Chapter 4 paras 4.3.1.1; 4.3.2.1; Chapter 5 paras 5.2.1; 5.3.2.1; 5.3.4.2; and 5.5.1.1. For referred legislative texts see, Guide to UNCITRAL Model Law para 79; E-commerce Directive art 9; CRD art 1, AU Convention arts 2 & 5; SADC Model Law s 10; EAC Framework Phase 1 r 6; and the ECOWAS E-transactions Act art 20.

8 See Chapter 3 para 3.3.2.2; Chapter 4 para 4.3.1.1; Chapter 5 paras 5.3.2.1 and 3.3.4.1. See specifically UNCITRAL Model Law art 13; SADC Model Law s 16 and the EAC Framework Phase 1 r 6.

- Parties are at liberty to agree on their own contract terms, including choosing an applicable law and the court which will be seized of jurisdiction.[9]
- Terms and agreements in documents which are referred to outside the contract document itself, are binding on the parties provided that reference to the external document is sufficiently conspicuous to be noticed by the parties.[10]
- A contract may be concluded online by means of an offer and its acceptance by the offeree. To validate a contract online, an offeree should be able to review the details of his or her order before confirmation. The act of confirmation is an acceptance of the offer...[11]
- A message is deemed to have been sent when it leaves the information system of the originator and is no longer under his or her control, and then enters a designated information system of the recipient, or, if there is no designated system, when it is retrieved by the recipient.[12]
- A message is regarded as having been received when it enters the information system of the recipient, provided that there is no presumption of law that what was received is the same as what was sent.[13]
- Where an originator requests an acknowledgement of receipt of a communication as a condition for indicating receipt, that communication will only be

9 See Chapter 3 para 3.3.2.3 and Chapter 5 paras 5.2.1; 5.3.2.1; 5.3.4.1; and 5.5.1.1. On referred legislative texts see Guide to UNCITRAL Model Law para 79; AU Convention arts 5-6; SADC Model Law s 11; EAC Framework Phase 1 r 3 and ECOWAS E-transaction Act art 35.

10 For a detailed discussion see Chapter 3 para 3.3.2.2; see also Chapter 5 paras 5.3.2.1; 5.4.3.1; and 5.4.3.1. See further, UNCITRAL Model Law art 5bis; SADC Model Law s 9; and the EAC Framework Phase 1 r 6.

11 See Chapter 3 para 3.3.2.3; Chapter 5 paras 5.2.1 and 5.5.1.1. See also UN CITRAL Model Law art 11; AU Convention art 5 and ECOWAS E-transaction Act art 20.

12 See Chapter 3 para 3.3.2.3; Chapter 5 paras 5.2.1 and 5.5.1.1. For legislative texts see UNCITRAL Model Law art 11; AU Convention art 5; and ECOWAS E-transactions Act art 20.

13 Although this position can be argued in that, where a document is deemed sent it appears more logical within the tenets of law, to presume that what was sent is equal to what was received. The onus should be on the recipient to show that what was received differs from what was deemed sent; see the discussion in Chapter 3 para 3.3.2.3 and Chapter 5 para 5.3.2.1.

deemed to have been received when the recipient sends the acknowledgement.[14]

- A communication is received at the place where the recipient has his or her place of business, and if there is no place of business, at his or her habitual place of residence.[15]

- Suppliers are obliged to provide basic information on their business; name; contact details (physical address, e-mail and phone number); registration information; codes of subscription (if any); dispute resolution processes; confirmation procedure; after-sales services; privacy rights; cancellation rights, periods and processes; payment options; and policies on refunds.[16]

- Information requirements regarding the goods must include all forms of charges, including transportation, taxes, cost of return, charges on communication during enquiries, and a proper description of the goods and their functionality, where applicable.[17]

- In the event that goods are returned, consumers are liable for the cost of returning the goods unless there is an arrangement by the supplier for a more expensive means of returning the goods, in which case, the supplier will be liable for the difference.[18]

- In jurisdictions where the right to withdraw without reason is available, that right does not extend to contracts for consumables and daily supplies; personalised

---

14 See Chapter 4 para 4.3.1.1; Chapter 5 paras 5.2.1 and 5.5.1.1. See further, E-commerce Directive art 11; AU Convention art 5 and ECOWAS E-transactions Act art 28.

15 This conclusion is drawn from the discussions in Chapter 3 para 3.3.2.3; Chapter 5 paras 5.3.2.1; and 5.3.4.1. See further, UNCITRAL Model Law art 15; SADC Model Law s 14 and EAC Framework Phase 1 r 9.

16 The different legislative texts and documents insist on the supplier's information in order to demystify anonymity on the internet see discussions in Chapter 4 paras 4.2.1.1; 4.3.1.1; 4.3.2.1; Chapter 5 paras 5.2.1; 5.3.2.1; and 5.5.1.1. Legal texts which were discussed in the paragraphs include CPR paras 4 & 10; E-commerce Directive art 10; CRD arts 6-8; AU Convention art 2; SADC Model Law s 25; and the ECOWAS E-transactions Act art 5.

17 See Chapter 4 paras 4.3.1.1; 4.3.2.1 with reference to CRD arts 6 & 22 and Chapter 5 para 5.2.1 with reference to art 2 of the AU Convention.

18 In South Africa and in the EU, there is a fixed time for withdrawing from or canceling a contract see Chapter 4 para 4.3.2.1 and Chapter 5 para 5.7.3.1(g).

goods; goods subject to price fluctuation; goods bought on auction; perishable items; or items that once opened cannot be returned.[19]

- Commercial communications[20] should be easily identified and should not bear misleading headings, and the natural or legal person on whose behalf the communication is made, should be made known.[21]
- Unsolicited commercial communications should include a free and easy-to-access, opt-out process irrespective of prior consent in regions where the law so requires.[22]
- Inertia selling, or the sale of unsolicited goods, is prohibited and consumers are not liable to pay, return, or pay for any damage to such goods.[23]
- Consumers are entitled to performance within a limited period based on agreement; and if there is no agreed time for delivery, performance should be within a reasonable period. Failure to perform a contract within a reasonable time, entitles the consumer to withdraw from the contract or to a refund of his or her money if payment has been made.[24]
- There is a limitation on the liability of ISPs in online transactions for third-party content, provided they only play technical roles of catching, transmitting or linking. Where there is an infringement, take-down notices are to be issued on the

19 See Chapter 4 para 4.3.2.2 and the CRD art 16; see further Chapter 5 para 5.3.2.2 with reference to the SADC Model Law s 27; para 5.4.1.1, and the COMESA Model Law art 22.

20 Commercial communications could be direct or indirect. A direct communication is a communication which is specifically sent to a recipient and that form of communication could also be referred to as unsolicited commercial communication. On the other hand, an indirect commercial communication is akin to an invitation to treat, is addressed to the whole world, and is not sent to a specific recipient, such as information or advertisements on a web-site.

21 See discussion on this in Chapter 4 para 4.2.1.1 CPR paras 4 & 10 and Chapter 5 paras 5.2.1 and 5.5.1.1 with reference to AU Convention art 4(6) and ECOWAS E-transactions Act art 8.

22 This is discussed in Chapter 4 para 4.3.1.1(c), with reference to art of the CRD; see also, Chapter 5 para 5.3.2.1 SADC Model Law s 30.

23 See Chapter 4 para 4.3.2.1 CRD art 27.

24 For an insight into this conclusion see Chapter 4, paras 4.2.2.1; 4.3.2.1; Chapter 5 paras 5.3.2.1; 5.3.4.1; 5.4.1.1; and 5.5.1.1. Referenced sources include CRD arts 18-19; SADC s 26; EAC Framework Phase 1 r18; COMESA Model Law art 24 and the ECOWAS E-transactions Act art 6.

ISPs to forestall such infringements.[25] In that case they are not liable to third parties for the removal of illegal contents upon receiving a take-down notification. ISPs are also under no obligation to monitor as this may be impracticable. But where they are found to have been involved in or aware of illegal activities on the sites they are hosting, they will be liable to that extent.

- In virtually all the jurisdictions whose e-transaction laws were studied, there was a common choice-of-law clause. Most of the national laws provide that, irrespective of the law which will apply to the transaction, it will only be enforceable against their nationals if it provides substantially similar protection and rights to the party as are provided in their national legislation.[26]
- In addition to court processes, the use of ADR or ODR is encouraged in that it is more accessible, cheaper, faster, and convenient and guarantees a win-win situation.[27]

From these principles, certain consumer rights were identified: the right to information; the right to withdrawal and cancellation; the right to a refund; the right to timely performance; and the right to a safe payment system. Suppliers or providers are liable to the consumers whenever any of these rights are breached.

The above notwithstanding, some other principles were found in the CRD,[28] these principles are not widespread and will be discussed under the paragraph on recommendations.

---

25 South Africa has a well laid out procedure for a take-down notice see Chapter 5 para 5.7.3(1)h. above on the extent of liabilities of ISPs see Chapter 4 para 4.3.1.1; Chapter 5 paras 5.3.2.1; and 5.3.4.1. See further, E-commerce Directive arts 12-13; SADC Model Law ss 31-34; and the EAC Framework Phase 1 r 11.

26 See s 109 UCITA and s 30(4) Nigerian E-transactions Bill.

27 See Chapter 3 para 3.4; Chapter 4 para 4.2.1.1; 4.3.1.1; 4.3.2; 4.3.4 and Chapter 5 para 5.4.2. See also UNCP Guidelines para 4; E-commerce Directive art 17; Directive on Better Enforcement and Modernisation art 5; Directive on Consumer ADR arts 5 & 26 and COMESA Model Law art 30.

28 For instance the CRD protects consumers from paying additional costs outside the stat-

9.2.2 Conclusions from international, regional and national instruments

In the preceding chapters, legislative texts of the UN, EU, OECD, and Africa on e-transactions were studied; from them the following conclusions can be drawn.

(a) Divergent laws on e-transactions would impede the growth of e-commerce and constitute a barrier to consumer protection.[29]

(b) There is agreement as to the need for harmonisation of e-commerce regulations at regional level in line with international best practices and in cooperation with international bodies.[30]

(c) Although none of the legislative texts offered exactly the same level of protection for consumers, most basic principles were modelled on the UNCITRAL Model Law and these principles ran across the different legislative texts and instruments with some measure of uniformity.[31]

(d) In the EU it can be asserted that there is some level of certainty in e-commerce regulations. There are also centralised and national agencies responsible for enforcement and consumer redress. As has been earlier noted, determining the jurisdiction which will be seized of consumer contracts is well articulated and is predictable in the EU.[32]

(e) In Africa, the COMESA Model Law and the EAC Framework Phase 1 attempt to harmonise their legislative texts with those of the UNCITRAL Model Law and the EC Convention, and take further steps to include consumer rights in their

---

ed costs which suppliers provide on their websites see chapter 4 para 4.5.1(c) and arts 19, 21 and 22 of the CRD. The CRD further provides for the use of mobile phones and devices with limited space for e-commerce and requires that software is compatible with any device in which it is installed, see CRD art 6 (r) and (s).

29 See Chapter 4 paras 4.1; 4.3.2.1 and art 4 of the CRD. See further, Chapter 5 para 5.1.

30 See Chapter 4 para 4,3.2.1; Chapter 5 paras 5.1 and 5.3.2.4.

31 For instance, among the regional instruments in Africa the SADC Model Law; COMESA Model Law and the EAC Framework Phase 1 are modeled after the UNCITRAL Model Law see Chapter 5 paras 5.2; 5.3.2.1; 5.3.5.4; and 5.4.1. See similarly, the Australian ETA in Chapter 4 para 4.5.3. The influence of the UNCITRAL Model Law is also obvious in the US through the UETA, see Chapter 6 para 6.2.1.

32 See Chapter 4 para 4.6.

legislation while also extending the scope of their law to apply to both businesses and consumers. In most parts of Africa there is, however, no specified period within which a consumer may withdraw from an e-contract. There are also no functional and well-established consumer protection agencies responsible for resolving consumer disputes. With the exception of the COMESA, the dispute resolution system for consumer issues has not received much thought or been widely implemented. There are also no practical arrangements for the establishment of enforcement agencies in most of the African regional instruments. In the absence of a monitoring and enforcement agency, consumer protection will not be effective. The AU Convention, which has only recently been adopted, leaves much to be desired. It is, however, a first step in the right direction and the Convention is still open to amendment. Also, the ECOWAS Supplementary Act on E-transactions builds on the AU Convention thus sustaining harmonised principles, although the Act has not improved substantially on the AU Convention. On the whole, it is submitted that the level of protection for consumers in Africa is relatively low and largely inadequate.[33]

(f) There is no online platform for consumer redress in most of the texts. In the EU, the CRD elaborates on a general redress system and procedure. This system has been captured under the EU Directive on Consumer ADR and includes both face to face and online dispute resolution methods. In Africa, there is no provision on dispute resolution which exceeds the arrangements made under the COMESA Model Law. The COMESA Model Law provides, implements, and sets out conciliation rules for the proper functioning of a consumer-redress system. The system provides for alternative dispute resolution with a conciliation process that can be managed electronically.[34]

33 For an insight into this discussion see Chapter 5 paras 5.2.1; 5.3.1 and 5.4.1.

34 See Chapter 5 para 5.4.2 on the procedures for online conciliation under COMESA.

(g) Save for the CRD there is little or no provision for the protection of consumers who buy auctioned products online, or for users of digital contents and m-consumers.[35]

(h) Not all the provisions of the EC Convention apply to consumers, and most of the provisions of the UNCITRAL Model Law are no longer adequate to address the different issues arising in e-commerce and consumer protection.[36]

(i) The texts are technology-neutral and do not make mandatory specifications on applicable technologies for different processes.[37]

(j) Taking all the international, regional and national instruments together, it is safe to conclude that the consumer protection principles contained therein are not comprehensive enough.[38]

9.3 Recommendations

The recommendations made here are geared towards having comprehensive rules, which will place e-commerce consumers at par with conventional consumers and at the same time offer a harmonised level of protection to consumers globally. In addition to expanding the extant consumer-protection principles which have been identified, there are recommendations of other principles which could be enacted to fill some gaps as well as address recent technological advancements. These recommendations should be captured in a single instrument in the form of a Convention. Furthermore, the recommendations should of necessity be contained and implemented in national laws across borders in order to provide a certain level of adequate protection for e-commerce consumers. The recommendations are in what follows.

---

35 Consumers in the EU are protected during online auction sales see Chapter 4 para 4.3.2.1; see further, CRD Recital 24.

36 See Chapter 3 paras 3.2 and 3.6.

37 For a discussion on this, see Chapter 3 para 3.2; Chapter 5 paras 5.3.2.1; 5.3.4.1; Chap ter 6 para 6.2.1. See further Preamble to EC Convention para 46; Preamble to SADC Model Law para 5; EAC Framework Phase 1 r 14; and UETA s 7(d).

38 See Chapter 3 para 3.6; Chapter 4 para 4.6; Chapter 5 para 5.8; Chapter 6 para 6.9; and Chapter 8 para 8.6.

9.3.1 Recognition and validity of electronic transferable records

To date transactions are generally governed by written documentation. However, with advances in technology, the law had to provide a functional equivalent of paper through the recognition and validation of data messages. However, technology evolves and creates new opportunities for which the law should continue to provide for. The recognition of data messages does not specifically include transferable records in all jurisdictions; neither does most e-transaction related legislation address issues that are akin to the use of e-transferable records. With the UNCITRAL Model Law on e-transferable records, the issues specific to the adoption of an electronic equivalent of a transferable record are legally recognised. Its use across all jurisdictions at the national level should therefore be implemented through legislation.

It is therefore proposed that:

- The nature of title documents that can be electronically presented should be specified in e-transaction instruments.
- The legal rights and recognition which accrue from the use of transferable records should also accrue to the holder of an e-transferable record.

9.3.2 Provision overriding unfair terms

The inclusion of what amounts to unfair terms in e-commerce consumer contracts is crucial to consumer protection. From what is seen, most e-transaction legislation does not deal with the issues of unfair terms and their unenforceability.

It is therefore proposed that:

- Unfair terms should be identified and included in e-transaction legislation unless distinct and comprehensive legislation on unfair terms which are particularly relevant to e-commerce already exists. Where there is none, it would be appropriate to include rules on unfair terms as a guide to both consumers and suppliers in order to help the parties to understand their rights and limitations. It is trite

law that unfair terms in a contract are regarded in the courts as unconscionable and are, therefore, not enforceable against the consumer. The contract may not necessarily be nullified in its entirety if it can be performed wholly or in part, irrespective of the unfair terms.[39]

9.3.3 Prohibition of unsolicited commercial communications

Tempted by the range of consumers that could be reached directly and cheaply at the same time, spam and telemarketing offer an interesting vista for suppliers. Spam undoubtedly increases the use of data and entails loss of man-hours for the consumer. The use of dictionary attacks, data profiling, and the sale of personal information, have over time encouraged spam, telemarketing, and inertia selling. The availability of consumer's information through data pass or similar means raises security and privacy issues, and leads to an abuse of personal information and, at times, fraud and identity theft. Unfortunately, these forms of unsolicited communication have not been totally banned in certain of the jurisdictions studied. The use of "Do-not-call/send Registries" notwithstanding, spam is on the increase. Some of these laws appear to be spam-tolerant as a result of the adoption of the opt-out approach which allows unsolicited communication provided the sponsors offer an easy and cost-free opt-out facility. An opt-in approach is rather advocated.

It is therefore proposed that:

- Unsolicited commercial communications should be prohibited outright and violations should be subject to punitive sanctions.
- No communication should be made to recipients without prior and express consent.
- Subsequent communications based on prior consent must be in respect of related goods or services and from the same originator only.

[39] For a thorough discussion of what constitutes unfair terms see Chapter 4 para 4.4.4.

- Every communication which is based on prior consent must provide an easy and cost-free unsubscribe option.

- There should be cross border co-operation through international and regional agreements in enforcing anti-spam rules against foreign spammers where no convention exists for global consumer protection and e-commerce.

9.3.4 Rules on dispatch and receipt

The general rule in the dispatch of e-communications is modelled on the UNCITRAL Model Law. The dispatch of an e-communication occurs when it enters an information system beyond the control of the originator or of the person who sent the e-communication on behalf of the originator.[40]

It is therefore proposed that:

- E-mail offers should have expiry dates; for instance every specific offer should have a life span after which the offer ceases if it was not acted upon.
- There should be the use of acknowledgment by a recipient as a condition for indicating receipt of a communication from the originator. This will resolve any conflict between the rules governing instantaneous and postal communications.
- Proof that a communication has been dispatched should raise an irrebuttable presumption of law that the e-communication sent is the same communication received by the recipient.

9.3.5 Cooling off and withdrawal periods

In view of the nature of e-transactions, consumers are limited in their decision-making process when they make online orders. A withdrawal period is therefore essential to

40 SADC Model Law s 12; see also UNCITRAL Model Law art 15.

balance the interests of consumers and to make up for some of the disadvantages they may suffer.

It is therefore proposed that:

- Every national law should make provision for a cooling-off and withdrawal period. The period should be harmonised so as to provide certainty for consumers and suppliers without the restriction of researching into different national laws in order to ascertain how long consumers may take before their orders become final under different national laws.

9.3.6 Procedure for take-down notifications

Where there is infringing or offensive information on the internet, the provider of that particular service may, by a take-down notice, be obliged to remove such content from its server. Direct notices from individuals should not be honoured as such a practice may become abusive. However, the procedure for the take-down notices has not been well established, save in countries like South Africa where the ECTA provides a detailed procedure for a take-down notice.

It is therefore proposed that:

- ISPs should be able to remove offensive content from their sites upon receipt of a take-down notice issued by a court, or preferably by an agency considering the procedures and delays that are customary in court processes. Learning from the ECTA, individuals who request take-down notices must not be anonymous and must accept responsibility for their actions.[41]

9.3.7 Online auctions

Online auctions are another area of electronic trading which generates a large number of consumer complaints. Most common complaints refer to goods not delivered to buyers or payment not made to sellers. Consumers also face problems with redress

[41] Section 77 of the ECTA; see also Chapter 5 para 5.7.3.1(h).

because the auction sites do not accept liability for sellers' or buyers' losses, or for the quality, safety, or legality of the products on sale. Examples of these sites include the eBay and eBid.[42] The UK Office of Fair Trading[43] reported that the required information about business sellers at an auction sale is not always available to consumers, and that consumers often do not know whether they are dealing with a seller selling in the course of a business or not.

The online-auction challenge is further exacerbated by the fact that consumers cannot exercise withdrawal rights or rights to a refund in online auctions.[44]

It is therefore proposed that:

- Rules on internet auctions, including eBay-style auctions, should be provided for in legislation and made enforceable against the parties. Special monitoring obligations should be imposed on business sites that offer auction sales in order to enforce performance.
- Consumers should be entitled to exercise the right to a refund in online auctions, subject, however, to proof of poor quality or non-performance.

9.3.8 Technological advances

Technological advances have ensured that the way in which the internet is accessed has improved over the years. The use of single-window facilities – especially the mobile device – is increasingly replacing the functions of a computer. There are new issues germane to this development and, as was noted in Chapter 1, law is evolving and must follow change. The widespread use of the mobile phone has also improved the sale of digital products, services, and streaming media. Aggressive reliance on digital goods raises the question of operability, which the law should address across the board. Challenges arising from the use of mobile devices are myriad and both

42 Office of Fair Trading *Internet Shopping An OFT market study* (2007) available at https://webarchive.nationalarchives.gov.uk (date of use: 08 March 2019) 136.

43 Office of Fair Trading *Internet Shopping An OFT market study* (2007) 135.

44 See the CRD art 16(k).

technical and legal. Technically, the screens are small and adapted to display limited information and on a single screen or window. Not all information displays correctly on a mobile browser, and this limits the amount of information that may be available to the recipient of a service. If it is borne in mind that one of the keys to consumer protection is adequate information, then it becomes clear that the inadequacies inherent in the use of a mobile device in e-commerce present a threat to consumer protection. Nonetheless, as has been provided in the CRD, suppliers using the mobile platform for their sales should make as much information as possible available to the recipient, bearing in mind the limited size of the screen.

In the OECD Policy Guideline on emerging consumer protection,[45] it is suggested that where the suppliers cannot make all the relevant information available, consumers should be referred to a webpage where they may access complete information. It is recommended that consumers should not stop at accessing the webpage, but should be compelled to click on a button which would show that the page had been accessed, and without which they would not be able to proceed with the transaction.

It is therefore proposed that:

- Due to the increased use of digital products and services, there should be information on any relevant interoperability of digital content with hardware and software that the trader is aware of, or of which it can reasonably be expected to be aware.
- There should be information on the technical aspects of, and technical protection measures available for digital content, as well as information on the existence of and conditions governing after-sale customer assistance and after-sale services, where applicable.
- Additional information requirements describing the main characteristics of goods or services and compatibility of software which consumers may want to download to their hardware should be specifically made available for users of

45 OECD Policy Guidelines for Addressing Emerging Consumer Protection at 6.

m-devices in e-transaction and consumer protection laws at both the regional and national levels.[46]

- Users of mobile devices should be made to pass through stringent confirmation procedures, such as having to confirm their orders using their e-mail. This process is similar to a double verification or two factors verification process which is already in use prior to accessing certain services online. This way, identity theft and input errors would be reduced, and the e-mail would also serve as a means of durable storage of the confirmation page.
- In order to minimize over-consumption, there should be a threshold or expenditure limit on lines that are registered to under-age users with the written consent of their guardians.
- Mobile operators should monitor the activities of mobile vendors and aggregators who trade through their networks in order effectively to identify them and make their locations and information available to subscribers in the event of defective performance, fraud, refunds, complaints, opting-out, and dispute resolution. This can be achieved by expanding the scope of their regulations and terms of use with third parties and other users.

9.3.9 Data protection

Data protection is an aspect of the law that has in recent times received intense attention. Many countries are sensitised and have enacted data protection legislation. Privacy policies are readily visible on standard websites, but where there are no laws, those policies cannot be enforced. Despite internet trade and interaction, some countries are data havens with no comprehensive data-protection legislation. Although most of the countries which were studied to this point, did not have data-protection or

46 See for instance CRD art 6.

privacy-specific provisions in their e-transaction law, they, however, have distinct data-protection legislation in place. [47]

It is therefore proposed that:

- In countries where there is no specific data-protection legislation, consumer-protection - related issues regarding privacy should be included in the country's e-transaction legislation. Without this the privacy of consumers could be infringed through data collected by vendors or service providers in the course of business.

9.3.10 Security of payment systems

There are security issues involved in e-payment systems, including: payment into and from wrong accounts; excess payment, especially resulting from input errors; fraudulent use of payment cards[48] and subsequent unauthorised payments; and the unauthorised use of account information. There is provision for correction of errors in e-transactions by withdrawing the portion of the error and notifying the other party as soon as possible. [49] Charge-back systems are also available in the event of cancellation or other demands.

It is therefore proposed that:

- In countries where there is no specific protection for users of the electronic wallet, the e-transaction law in that country should provide for rules governing the obligation of payment providers to apply safe payment options, and to make information available to consumers before, during and after the use of any payment method. Payment providers should also provide easy means for

47 For instance, Australia, UK, US and 96 per cent of European countries have distinct data protection legislation while in South Africa, e-transaction and data protection rules are contained in the same legal instrument. In Africa, 52 per cent of African countries have data protection legislation either as a separate piece of legislation or contained in a comprehensive legislation which provides for e-transaction, consumer protection, data protection and sometimes, cyber security, see UNCTAD "Data protection and privacy legislation worldwide" available at www.unctad.org (date of use: 06 June 2021).

48 Directive 97/7/EC on Consumer Protection art 8.

49 SADC Model Law s 16(2).

deactivating cards or wallets in the event of theft or fraud. They should clearly state conditions for refunds and chargeback and the processes involved. A complaint and settlement procedure should be well defined under payment schemes.

- Consumers should be protected from payment of additional fees in respect of the use of a specified payment option involving fees exceeding the regular fees or charges.[50]

9.3.11 Alternative/online dispute resolution

The benefits of alternative dispute resolution in conventional settings and through an online platform – otherwise known as online dispute resolution – have been identified in some texts[51] and need to be enshrined in all e-transactions legislation. Another laudable move which simplifies the handling of consumer complaints is that certain jurisdictions have established agencies which handle consumer complaints and address consumer issues, a process akin to a class action.

Again, disputes could be resolved online through electronic courts or virtual courts. Projects on cyber courts or virtual courts have been established in states such as Michigan,[52] and North Carolina[53] both in the US. Virtual court is a growing trend that should apply worldwide.[54]

It is therefore proposed that:

- A cyber-court, alternative dispute resolution centre, and an online platform for consumer redress to which all service providers, network providers, online mer-

50 CRD art 19.
51 See art 17 E-commerce Directive.
52 Viscasillas "Michigan creates cyber court" (2002) available at https://cio.com (date of use: 15 October 2020).
53 North Carolina Judicial Branch "Business Court Technology" available at https://www.nccourts.gov (date of use: 20 October 2020).
54 Niescier ed "Virtual courts and the future of personal jurisdiction" (2012) available at https://www.jurist.org (date of use: 20 October 2020).

chants, mobile operators, mobile vendors, and consumers will respond, need to be established both centrally and nationally. Sites subject to such a redress arrangement should be so indicated so that consumers can choose sites on which they wish to trade.

9.3.12 Implementation and enforcement agencies

Consumer protection principles, however enriched, will not achieve the desired objective in the absence of established and effective consumer protection centres which have implementation and enforcement powers.

It is therefore proposed that:

- An effective redress centre should be established both centrally and nationally with the capacity to impose and enforce sanctions, compensation orders, and other forms of punishment on infringing parties wherever their location.
- In line with the OECD recommendations discussed in Chapter Four of this study, cross-border cooperation should be highly coordinated across the globe.

9.3.13 Consumer education

Consumer education is key to mobilising consumers to become self-assertive. This can be achieved principally through the concerted efforts of consumer organisations. Organisations involved in consumer protection include “Consumers International” and the “International Chamber of Commerce” (ICC). Consumers International was founded in 1960 and supports, links, and represents consumer groups and agencies all over the world. It has a membership of some 200 organisations in almost 100 countries.[55] It strives to promote a fair society through defending the rights of the consumer. The other organisation, the ICC, hosts the ICC International Court of

[55] Consumers International “About Consumers International and our members” available at https://consumersinternational.org (date of use: 20 October 2020).

Arbitration and has developed dispute resolution platforms for both B2C and B2B e-commerce transactions.[56]

It is therefore proposed that:

- There should be massive education drive for consumers spearheaded by consumer protection groups in collaboration with international, national, and local agencies to sensitise consumers to their rights and available options when contracting online.

9.3.14 Jurisdiction

Critical among e-transaction issues, is the determination of jurisdiction in terms of applicable law and choice of forum where parties to a contract fail to agree on a choice of law before or after the conclusion of the contract. International private law provides rules of jurisdiction, choice of law, and recognition and enforcement of foreign judgments, for cases where there is a foreign element in the facts of the dispute.[57]

In the US,[58] it has become possible to establish that in e-contracts the choice of forum is that of the consumer, provided the supplier has targeted the jurisdiction of the consumer. This position does not differ substantially from that in the EU as the Brussels Regulation allows the consumer to sue the defendant in the consumer's jurisdiction or in that of the defendant, provided that the defendant has intentionally directed his or her activities to the consumer's jurisdiction. These approaches have been adopted in Nigeria through the E-transactions Bill.[59]

It is submitted that an international convention on jurisdiction which specifically addresses e-transaction issues will clear grey areas in jurisdiction in cross border e-transaction and further minimize the challenge of forum shopping.

---

56 ICC "Dispute resolution" available at https://iccwbo.org (date of use: 20 October 2020).
57 Anton *Private International Law* 1.
58 See Chapter 6 para 6.7.
59 See Chapter 8.

It is therefore proposed that:

- In the absence of an express agreement between the parties, there should be a universal rule conferring jurisdiction in e-transactions on the location of the consumer irrespective of where the transaction took place. To achieve this, there should be clear rules on how to determine the location of a consumer prior to entering into the contract, for instance, by the consumer, indicating a permanent address.

9.3.15 Harmonisation

In an attempt to address the adaptation of legal rules in a paper world to modern technologies, UNCITRAL was mandated[60] to prepare uniform private-law standards for e-commerce. This resulted in the UNCITRAL Model Law on E-commerce. In doing this, factors such as the borderless nature of e-commerce and its use even in jurisdictions without e-commerce laws were considered and this led to a conclusion that an international solution would benefit consumers more than a domestic based approach.[61] International harmonisation has been accepted as the logical approach to follow in addressing the legal implications of technological developments. International harmonisation helps to avoid barriers to international e-commerce arising from conflicting domestic standards,[62] and helps to foster economic growth.[63] According to Gillies, amongst other gains, "given the global, dematerialised nature of electronic commerce, a universal, harmonised approach would facilitate the modification of jurisdiction and choice of law rules."[64] Harmonisation is further seen as the approach by which to deal "with the legal implications of technological developments as a result of 'markets' migrating from geographic space to cyberspace."[65]

It is therefore proposed that:

60 See Chapter 3 para 3.1.2.
61 Faria (2004) 16 *SA Merc LJ* 529.
62 Ibid.
63 Glatt (1998) 1/6 *International Journal of Law and Information Technology* 57.
64 Gillies *Electronic Commerce* 200.
65 Kobrin "Economic Governance in an Electronically Networked Global Economy" available at www.repository.upenn.edu (date of use: 18 October 2020).

- E-transaction rules which embody comprehensive and contemporary e-consumer protection principles should be harmonised and prepared as a convention.
- States should be encouraged, through participation in international conferences and meetings, to recognise the need to adopt and accede to such a convention.
- A comprehensive and contemporary convention on e-transaction should effectively address issues that are shrouded in uncertainty, harmonise existing rules, and break through the barriers of culture and geography to achieve effective consumer protection.

9.4 Conclusion

Throughout this study, the role of the UNCITRAL Model Law in the field of e-commerce has been emphasised. The success of the UNCITRAL Model Law is best measured by the fact that it has served as a model for the e-transaction laws of many countries.[66] There is also no denying that the UNCITRAL Model Law has succeeded in transcending the challenges posed by divergent economic capacity, legal heritage, and telecommunications.[67] However, this study has also shown that the UNCITRAL Model Law has become out-dated as a result of the emergence of new legal issues in information technology, coupled with its failure to adequately address e-commerce consumer protection issues.

The exposition of the legal framework of different regions and countries undertaken in the preceding chapters on consumer protection online shows that there is no single document that adequately provides the much-desired protection for consumers who transact online. Furthermore, existing standards in the protection of online users differ from country to country thus creating uncertainty. Therefore, the international

66 Howland (1997) 32/6 *European Transport Law* 703.
67 Ibid.

harmonisation of e-commerce rules and e-commerce consumer protection principles in the form of a convention will undoubtedly be a major achievement in the promotion of e-commerce and e-commerce consumer protection.

Such a convention should embody all the recommendations contained in this study to ensure that consumer protection principles are comprehensively captured. These embodied principles will fill all existing gaps, capture new technological developments, and provide adequate protection for consumers who transact online. Finally, a revision of the UNCITRAL Model Law on e-commerce is advocated especially as a convention.

BIBLIOGRAPHY

BOOKS & CHAPTERS IN BOOKS & CONFERENCE PROCEEDINGS

Adebisi *Fundamentals of Computer Studies*
Adebisi JA *Fundamentals of Computer Studies* (Expert Solutions Consult 2013)

Akhigbe *Data Protection Law in Nigeria*
Akhigbe IJ *The Legal Framework for Data Protection Law in Nigeria* Unpublished Dissertation UNISA (2010)

Aithal PS *Mobile Commerce*
Aithal PS *Mobile Commerce* (Srinivas Publishers Date unknown)

Aldaheff and Cohen "Functionality of value-added network providers"
Aldaheff A and Cohen M "Functionality of value-added network providers and their liability" in Buys R & Cronje F (eds) *Cyberlaw@SA* 2 ed (Van Schaik 2004)

Aldrich *Videotex*
Aldrich MJ *Videotex-Key to the Wired City* (Quiller Press, London 1982)

American Law Institute *Restatement of the Law*
American Law Institute *Restatement of the Law Torts* 2d (Shop ALI Publications 1977)

Anton *Private International Law*
Anton EA *Private International Law* 2 ed (W Green 1990)

Arno "European Union"
Arno LR "European Union E-commerce Directive-article by article comments" in *EU regulation of e-commerce. A commentary* (Elgar commentary series 2017) 15-58

Asafe, Adebayo and Olalekan *Data Communications and Networking*
Asafe NY, Adebayo AF and Olalekan B *Data Communications and Networking* (Hasfem Nigeria 2015)

Atiyah *Essays on Contract*
Atiyah PS *Essays on Contract* (Oxford University Press 2012)

Ayeni *et al Computers in Society*
Ayeni RO et al *Computers in Society* (National Open University of Nigeria 2013)

Badaiki *Consumer Protection*

Badaiki AD *Consumer Protection and Standard Form Contracts in Nigeria* (Christdom 1999)

Baum and Perrit *Electronic Contracting*

Baum MS and Perrit HH *Electronic Contracting, Publishing and the EDI Law* (Wiley Law Publications 1991)

Bueker *et al IBM Security Solutions*

Buecker A *et al IBM Security Solutions Architecture for Network, Server and End-point* (IBM Redbooks 2001)

Burstein "A Global Network"

Burstein M "A Global network in a Compartmentalised Legal Environment" in Boele-Woelki K and Kessedjian C (eds) *Internet: Which court decides which law applies?* (Proceedings of the International Colloquium 2003) 23-34

Buys and Rothmann "Internet Law and Regulation"

Buys R and Rothmann J "Internet Law and Regulation" in Buys R & Cronje F (eds) *CyberLaw @ SA-the law of the Internet in South Africa* 2 ed (Van Schaik 2004) 393-422

Casterfranchi

Casterfranchi C "Guarantees for Autonomy in cognitive Agent Architecture" in *ECAI-94 Proceedings of the Workshop on Agent Theories, Architectures, & Languages on Intelligent Agents* (Springer-Verlag Berlin Heidelberg 1995) 56-70

Cate, Cullen and Mayer-Schonberger *Data protection principles*

Cate FH, Cullen P and Mayer-Schonberger V *Data protection principles for the 21st century* (2014)

Christie and Bradfield *Law of Contract*

Christie RH and Bradfield GB *Christie's The Law of Contract in South Africa* 6 ed (LexisNexis 2011)

Clark *Product Liability*

Clark AM *Product Liability, Modern Legal Studies* (Sweet and Maxwell London 1989)

David and Nicholas *Banking Litigation*

David W and Nicholas E (eds) *Banking Litigation* (Sweet & Maxwell 1999)

Delong and Froomkin "The next Economy?"

Delong JB and Froomkin AM "The next Economy?" in Hurley D, Kahin B & Varian H *Internet Publishing and Beyond: The Economics of Digital Information and Intellectual Property* (MIT Press Cambridge Massachusetts 1998)

Derick "Online banking law and payment systems"
Derick S "Online banking law and payment systems" in Buys R & Cronje F (eds) *Cyberlaw@SA 11* 2 ed (Van Schaik 2004) 227-314

Dicey, Morris and Collins *The Conflict of Laws*
Dicey, Morris and Collins *The Conflict of Laws* 15 ed (Sweet and Maxwell 2017)

Dinwoodie *Secondary Liability*
Dinwoodie GB ed *Secondary Liability of Internet Service Providers* (Springer 2017)

Downing and Covington
Downing D and Covington MA *Dictionary of Computer and Internet Terms* 8 ed (Barron's Educational Series 2009)

Eiselen "Purpose, Scope and underlying Principles of the UNECIC"
Eiselen S "The Purpose, Scope and underlying Principles of the UNECIC" in Anderson C & Schroeter UG (eds) *Sharing International Commercial Laws across National Boundaries: Festschrift for Abert H Kritzer on the occasion of his Eighthieth Birthday* (Wildy, Simmonds & Hills Publishing 2008) 106-133

Elegido *Jurisprudence*
Elegido JM *Jurisprudence* (Spectrum Law Series 1994)

European Commission *Comprehensive Approach*
European Commission *A Comprehensive Approach to Stimulating Cross-border e-Commerce for Europe's Citizens and Businesses* (2016)

Farrar and Dugdale *Introduction to Legal Method*
Farrar JH and Dugdale AM *Introduction to Legal Method* 2 ed (Sweet & Maxwell 1984)

Forouzan *Data Communications*
Forouzan B *Data Communications and Networking* 4 ed (Alan R Apt 2007)

Forsyth *Private International Law*
Forsyth CF *Private International Law: The Modern Roman-Dutch Law Including the Jurisdiction of the High Courts* 5 ed (Juta & Company Ltd 2012)

Furmstom *Law of Contract*
Furmstom MP *Cheshire, Fifoot and Furmston's Law of Contract* 12 ed (Butterworths London 1991)

Geist *Internet Law in Canada*
Geist MA *Internet Law in Canada* 3 ed (Captus Press 2002)

Gillies *Electronic Commerce*
Gillies LE *Electronic Commerce & International Private Law: A Study of Electronic Consumer Contracts* (Routledge 2008)

Gringas and Nabarro *Laws of the Internet*
Gringas C and Nabarro N *Laws of the Internet* (Butterworths London 1977)

Groth and Skandier *Network + Study Guide*
Groth D and Skandler T *Network + Study Guide* 4 ed (Sybex Inc 2005)

Guest *Chitty on Contracts*
Guest AG (ed) *Chitty on Contracts* 27 ed (Sweet & Maxwell London 1994)

Hance and Balz *Business and Law*
Hance O & Balz SD *Business and Law on the Internet* (McGraw-Hill 1997)

Harvey and Parry *Consumer Protection and Fair Trading*
Harvey B and Parry DL *The Law of Consumer Protection and Fair Trading* 6 ed (Butterworths London 2000)

Harvey *Internet.law.nz*
Harvey D *Internet.law.nz: Selected Issues* 4 ed (LexisNexis NZ Limited 2016)

Hay, Lando and Rotunda "Conflict of Laws"
Hay P, Lando O and Rotunda RD "Conflict of Laws as a Technique for Legal Integration" in Capelletti M, Seccombe M & Weiler J (eds) *Integration Through Law: Europe and the American Experience* vol 1 (Walter De GruyterNew York 1986) 161-260

Ikhide *Consumer Protection Law*
Ikhide E *Consumer Protection Law* (New Pages Law Publishing Co 2004)

Information Systems Analysts and Consultants *Information Technology Terminology*
Information Systems Analysts and Consultants *Information Technology Terminology (*Winnipeg Technical College 2008)

Jennings and Wooldridge "Applications of intelligent agents"
Jennings NR and Wooldridge MJ "Applications of intelligent agents" in Jennings NR, Wooldridge MJ (eds) *Agent Technology* (Springer, Berlin, Heidelberg 1998) 3-28

Kazeem *Electronic contract formation*
Kazeem MA *Electronic contract formation and the Nigerian initiatives* (2005)

Kerr *Law of Contract*

Kerr AJ *The Principles of the Law of Contract* 6 ed (Butterworths 2002)

Kilian and Boss (eds) *Electronic Communications*

Kilian W and Boss A (eds) *The United Nations Convention on the Use of Electronic Communications in International Contracts* (Kluwer Law International 2008)

Kuner "Directive 2000/31/EC"

Kuner C "Directive 2000/31/EC-Directive on Electronic Commerce" in *Concise European IT Law* (Kluwer Law International 2006) 205-262

Lawack *Electronic Payment Systems*

Lawack V *Electronic Payment Systems in South African Law* (LLM thesis University of Port Elizabeth 1997)

Lawson *et al French Law*

Lawson FH *et al* Amos & Walton's *Introduction to French Law* 3 ed (Oxford Clarendon Press 1967)

Lloyd *Information Technology Law*

Lloyd I *Information Technology Law* 7 ed (Oxford University Press 2014)

Lloyd *Legal Aspects of the Information Society*

Lloyd I *Legal Aspects of the Information Society* (Butterworths 2000)

Lodder and Kaspersen *eDirectives*

Lodder AR and Kaspersen HWK *eDirectives: Guide to European Union Law on E-Commerce* (Kluwer Law International 2002)

Longley and Shain *Dictionary of Information Technology*

Longley D and Shain M *Dictionary of Information Technology* 2 ed (MacMillian Press 1985)

Loos "Right of withdrawal-Interoperability of Directives"

Loos MBM "Right of withdrawal-Interoperability of Directives" in Terryn E, Straetmans G & Colaert V (eds) *Landmark cases of EU consumer law. In honour of Jules Stuyck* 545-547 (Cambridge 2013)

Magnus *Global Trade Law*

Magnus U *Global Trade Law: International Business Law of the United Nations and UNIDROIT; Collection of UNCITRAL'S and UNIDROIT's Conventions, Model Acts, Guides and Principles* (Sellier European Law Publications 2004)

Magnus and Mankowski *Brussels 1 Regulation*

Magnus U & Mankowski P *Brussels 1 Regulation* (Walter de Gruyter 2007)

Margolis *Random House Dictionary*
Margolis PE *Random House Webster's Pocket Computer & Internet Dictionary* (Random House, Incorporated 1999)

Martor, Sellers and Pilkington *Business Law in Africa*
Martor B, Sellers DS and Pilkington N *Business Law in Africa: OHADA and the Harmonisation Process* (Kogan Page Publishers 2002)

Mann and Winn *Electronic Commerce*
Mann RJ and Winn JK *Electronic Commerce* 2 ed (Aspen Publishers 2005)

Meiring "Electronic transactions"
Meiring R "Electronic transactions" in Buys R & Cronje F (eds) *Cyberlaw @SA* 2 ed (Van Schaik 2004)

Microsoft Press *Microsoft Computer Dictionary*
Microsoft Press *Microsoft Computer Dictionary* 5 ed (Microsoft Press Washington 2002)

Monye *Consumer Protection*
Monye FN *Law of Consumer Protection* (Spectrum Books Limited 2005)

Mouloul *Harmonisation*
Mouloul A *Understanding the Organisation for the Harmonisation of Business Law in Africa* 2 ed (OHADA 2009)

National Academics of Sciences, Engineering & Medicine *An Assessment of ARPA-E*
National Academics of Sciences, Engineering & Medicine *An Assessment of ARPA-E* (The National Academies Press Washington DC 2017)

NOUN *Introduction to Computers*
National Open University of Nigeria (NOUN) *Introduction to Computers* CIT 104 (NOUN 2005)

NOUN *Wireless Communication*
National Open University of Nigeria (NOUN) *Wireless communication* 1 CIT 655 (NOUN 2003)

Oluwole *Nigerian Electronic Banking Law*
Oluwole O *Nigerian Electronic Banking Law* (Nonesuchhouse Publishers 2009)

Oxford English Dictionary
Oxford English Dictionary of the English Language 1991 ed (New York Lexicon Publications Inc 1992)

Pablo *Online dispute resolution*

Pablo C *Online dispute resolution for consumers in the European Union* (Routledge Research in IT and E-commerce Law 2010)

Pound *Interpretations of Legal History*
Pound R *Interpretations of Legal History* (Cambridge University Press 2013)

Pradeep and Paul *An Assessment of ARPA-E*
Pradeep KK and Paul TB eds *An Assessment of ARPA-E* (The National Academies Press 2017)

Raisinghani "Key factors and implications for e-government diffusion in developed economies" 2305
Raisinghani MS "Key factors and implications for e-government diffusion in developed economies" in Mehdi K-P (ed) *Encyclopedia of information science and technology* 2 ed (2009) 2305-2312

Reed and Angel *Computer Law*
Reed C and Angel J (eds) *Computer Law: The Law and Regulation of Information Technology* 6 ed (Oxford University Press 2007)

Reed *Internet Law*
Reed C *Internet Law: Text and Materials* 2 ed (Cambridge CUP 2004)

Ringdon ed *Dictionary of Computer*
Ringdon JC ed *Dictionary of Computer and Internet Terms* vol 1 (Eastern Digital Resources 2016)

Riodan *The Liability of Internet Intermediaries*
Riodan J *The Liability of Internet Intermediaries* (Oxford University Press 2016)

Rhoton *Wireless Internet Explained*
Rhoton J *The Wireless Internet Explained* (Digital Press 2001)

Rowland and Macdonald *Information Technology Law*
Rowland D and Macdonald E *Information Technology Law* 2 ed (Cavendish 2000)

Rowland, Kohl and Charlesworth *Information Technology Law*
Rowland D, Kohl U and Charlesworth A *Information Technology Law* 4 ed (Routledge 2012)

Sagay *Nigerian Law of Contract*
Sagay IE *Nigerian Law of Contract* (Spectrum Books Ltd 1998)

Santon *Fundamentals of Marketing*
Santon WJ *Fundamentals of Marketing* (Mcgraw-Hill Inc 1978)

Schlechtrein *Commentary CISG*
Schlechtrein P *Commentary on the UN Convention on the International Sale of Goods (CIGS)* 3 ed (Oxford University Press 2010 1998)

Schryen *Anti-spam measures*
Schryen G *Anti-spam measures: Analysis and design* (Springer-Verlag 2007)

Scott and Black Cranston's *Consumers and the Law (Law in context)*
Scott C and Black J Cranston's R *Consumers and the Law (Law in Context)* 3 ed (Cambridge University Press 2000)

Shaw *International Law*
Shaw MN *International Law* 4 ed (Cambridge University Press 1997)

Smith *Internet Law*
Smith G *Internet Law and Regulation* 4 ed (Sweet & Maxwell 2007)

Smits *Advanced Introduction to Private Law* 1
Smits JM *Advanced Introduction to Private Law* (Edward Elgar Publishing 2017)

Sparrow *Successful IT Outsourcing*
Sparrow E Successful IT *Outsourcing: From Choosing A Provider To Managing The Project* (Springer-Verlag London 2003)

Sprindler, Riccio and Van der Perre *Liability of Internet Intermediaries*
Sprindler G, Riccio GM and Van der Perre *A Study on the Liability of Internet Intermediaries* (EU 2007)

Sprowl and Maggs *Computer Applications in the Law*
Sprowl JA and Maggs PB *Computer Applications in the Law* (West 1987)

Stewart *Network Security*
Stewart M *Network Security, Firewalls and VPNs* (Jones & Bartlett Learning 2011)

Susskind *Challenges of Information Technology*
Susskind R *The Future of Law Facing the Challenges of Information Technology* (Clarendon Press 1998)

Tang *Electronic Consumer Contracts*
Tang ZS *Electronic Consumer Contracts in the Conflict of Laws* (Oxford and Portland, Oregon 2009)

Thomsen and Wheble *Trading with EDI*
Thomsen HB and Wheble BS (eds) *Trading with EDI: The Legal Issues* (IBC Financial Books London 1989)

Todd *E-Commerce Law*
Todd P *E-Commerce Law* 169-182 (Cavendish Publishers London 2005)

Turban, King and Lang *Introduction to Electronic Commerce*
Turban E, King D and Lang J *Introduction to Electronic Commerce* 3 ed (Pearson USA 2010)

Vagadia "Contract discharge and methods to reduce liability"
Vagadia B "Contract discharge and methods to reduce liability" in *Outstanding to India-A legal handwork* (Springer, Berlin, Heidelberg 2007) 73-80

Van der Merwe *et al Information and Communications*
Van der Merwe DP *et al Information and Communications Technology Law* 2 ed (LexisNexis 2016)

Van der Merwe *et* al *Contract: General Principles*
Van der Merwe S *et al Contract: General Principles* 3 ed (Juta 2007)

Van der Merwe *et al Contract: General Principles*
Van der Merwe S *et al Contract: General Principles* 4 ed (Juta 2012)

Van der Merwe *Computers and the Law*
Van Der Merwe *Computers and the Law* 2 ed (Juta 2000)

Walden *EDI and the Law*
Walden I *EDI and the Law* (Blackwell Publishers 1989)

Ward and Akhtar *Walker & Walker's English Legal System*
Ward R and Akhtar A *Walker & Walker's English Legal System* 11 ed (Oxford University Press 2011)

Weber *Economy and Society*
Weber M *Law in Economy and Society*, translated by Rheinstein (Harvard University Press 1954)

Woolridge and Jennings *Agents*
Woolridge M and Jennings NR (ed) *"*Agent theories, architectures, and languages" in ECAI-94 Proceedings of the workshop on Agent Theories, Architectures, and Languages on Intelligent Agents 1-39

Wright and Winn *Electronic Commerce*
Wright B and Winn JK *The Law of Electronic Commerce* 3 ed (Aspen Law & Business 1998)

JOURNAL ARTICLES

Adeyemi (2018) 24/1 *Computer and Telecommunications Law Review*
Adeyemi A "Liability and exceptions of intermediary service providers (ISPs): Assessing the EU electronic commerce legal regime" (2018) 24/1 *Computer and Telecommunications Law Review* 6-12

Akhigbe (2019) 6 *Benin Journal of Public Law*
Akhigbe IJ "Impact assessment of Nigeria laws on the protection of privacy of recipients of telecommunication services" (2019) 6 *Benin Journal of Public Law* 193-212

Akomolede (2008) 3 *PER*
Akomolede TI "Contemporary legal issues in electronic commerce in Nigeria" (2008) 3 *PER* 1-24

Alba (2013) 5 *Creighton International and Comparative Law Journal*
Alba M "Transferability in the electronic space at a crossroads: Is it really about the document?"(2013) 5 *Creighton International and Comparative Law Journal* 1-28

Aldrich (2011) 33/4 *Annals of the History of Computing*
Aldrich M "Online Shopping in the 1980s" (2011) 33/4 *Annals of the History of Computing* 57-61

Amro (2016) 20 *Vindobona Journal of International Commercial Law & Arbitration*
*Amro JI "*Theory and Practice of Cross-Border Electronic Commerce Transactions" (2016) 20 *Vindobona Journal of International Commercial Law & Arbitration 2-22*

Angel (1999) 2 *JILT*
Angel J "Why use digital signatures for electronic commerce?" (1999) 2 *JILT* 3-25

Army (2005) 33/4 *Pepperdine Law Review*
Army GM "Is spam the rock of sisyphus?: Whether the Can-Spam Act and its global counterparts will delete your e-mail" (2005) 33/4 *Pepperdine Law Review* 1021-1066

Bagraim (1998) 2/6 *Juta's Business Law*
Bagraim P "Transacting in cyberspace" (1998) 2/6 *Juta's Business Law* 50-54

Baistrocchi (2002) 19/3 *Santa Clara High Technology Law Journal*
Baistrocchi PA "Liability of intermediary service providers in the EU Directive on Electronic Commerce" (2002) 19/3 *Santa Clara High Technology Law Journal* 111-130

Barber and Edghill (2006) 24/4 *Communications Law Bulletin*
Barber S and Edghill B "E-commerce Developments" (2006) 24/4 *Communications Law Bulletin* 22-27

Bayer (2008) 1 *Victoria University of Wellington Working Paper Series*
Bayer J "Liability of internet service providers for third party content" (2008) 1 *Victoria University of Wellington Working Paper Series* 1-110

Bernstein and Ramchandani (2002) *Canadian Journal of Law & Technology*
Bernstein A and Ramchandani R "Don't shoot the messenger! A discussion of ISP Liability" (2002) *Canadian Journal of Law & Technology* 77-85 available at https://www.ojslibrary.dal.ca (date of use: 22 September 2018)

Beykirch (1998) IX *Magazin fur professionelle Informationstechnik*
Beykirch Hans-Bernhard "Weltweit Handeln-OTP: Open Trade Protocol" (1998) IX *Magazin fur professionelle Informationstechnik* 122-126

Blyth (2005) 11 *Rich JL & Tech*
Blyth SE "Digital signature law of the United Nations, European Union, United Kingdom and United States: Promotion of growth in e-commerce with enhanced security" (2005) 11 *Rich JL & Tech* 1-20

Boss (2001) 37/2 *Idaho Law Review*
Boss AH "The Uniform Electronic Transactions Act in a global environment" (2001) 37/2 *Idaho Law Review* 275-352

Burgess (1986) 15 *Anglo American LR*
Burgess A "Consumer adhesion contract and unfair terms: A critique of current theory and suggestion" (1986) 15 *Anglo American LR* 255-258

Cameron (2001) *Computers and Law*
Cameron B "Jurisdiction and the Internet" (2001) *Computers and Law* 13-21

Cauffman (2012) 19/1 *Maastricht Journal of European and Comparative Law*
Cauffman C "The Consumer Rights Directive adopted" (2012) 19/1 *Maastricht Journal of European and Comparative Law* 212-218

Chandler (1998) 22 *Tulane Maritime Law Journal*
Chandler GF "Maritime Electronic Commerce for the Twenty-first Century" (1998) 32/6 Tulane *Maritime Law Journal* 463-503

Chanin (1999) 18 *John Marshall J Computer & Information Law*
Chanin JA "The Uniform Computer Information Transactions Act: A practitioner's view" (1999) 18 *John Marshall J Computer & Information Law* 279-322

Christensen and Low (2004) 1 *Digital Evidence & Electronic Law Review*
Christensen S and Low R "Electronic signatures and PKI Frameworks in Australia" (2004) 1 *Digital Evidence & Electronic Law Review* 40-43

Coetzee (2004) 15/3 *Stellenbosch LR*
Coetzee J "The Electronic Communications and Transactions Act 25 of 2002: Facilitating electronic commerce" (2004) 15/3 *Stellenbosch LR* 501-521

Daniel (2004) *Santa Clara Computer and High Technology LJ*
Daniel JL "Electronic contracting under the 2003 revision to article 2 of the Uniform Commercial Code: Clarification or chaos?" (2004) *Santa Clara Computer and High Technology LJ* 319-346

Denning PJ *et al* (1989) 32/1 *Communications of the ACM*
Denning PJ *et al* "Computing as a discipline" 1989 32/1 *Communications of the ACM* 9-23 available at www.webcitation.org (date of use: 25 October 2019)

Dively (2000) 38/2 *Duquesne Law Review*
Dively MH "The new laws that will enable electronic contracting: A survey of the electronic contracting rules in the Uniform Electronic Transactions Act and the Uniform Computer Information Transactions Act" (2000) 38/2 *Duquesne Law Review* 209-254

Drigas and Leliopoulos (2013) 4/4 *International Journal of Knowledge Society Research*
Drigas A and Leliopoulos P "Business to consumer (B2C) e-commerce decade evolution" (2013) 4/4 *International Journal of Knowledge Society Research* 1-10

Donnie and William (2000) 26 *RCTLJ*
Donnie LK and William D "Adapting contract law to accommodate electronic contracts" (2000) 26 *RCTLJ* 215-276

Dugan (2001) *New Zealand LJ*
Dugan B "Electronic transactions: The quest for clarity" (2001) *New Zealand LJ* 483-488

Eiselen (1995) 7 *SA Merc LJ*
Eiselen S "The Electronic Data Interchange Agreement" (I995) 7 *SA Merc LJ* 1-18

Eiselen (1999) 6 *EDI LR*
Eiselen S "Electronic Commerce and the UN Convention on Contracts for the International Sale of Goods (CISG) 1980" (1999) 6 *EDI LR* 21-46

Eiselen (2007) 10 *PELJ*

Eiselen S "The UNECIC: International trade in the digital era" (2007) 10/2 *PER/PELJ* 48-95

Eiselen and Bergenthal (2006) 39 *CILSA*
Eiselen S and Bergenthal SK "The battle of forms: A comparative analysis" (2006) 39 *CILSA* 214-240

Elliot *Cambridge Law Journal* (2017) 76/2
Elliot M "The Supreme Court's judgment in Miller: In search of constitutional principle" (2017) 76/2 *Cambridge Law Journal* 257-288 available at https://www.repository.cam.ac.uk (date of use: 15 October 2019)

Eseyin and Chukwuemeka (2018) 72 *Journal of Law, Policy and Globalization*
Eseyin M and Chukwuemeka CW "Articulating Consumer's Rights as Human Rights in Nigeria" (2018) 72 *Journal of Law, Policy and Globalization* 124-132

Esselaar and Miller (2002) 2/1 *SAJIC*
Esselaar P and Miller L "Towards electronic commerce in Africa: A perspective from three country studies" (2002) 2/1 *SAJIC* 1-12 online version available at https://journals.co.za (date of use: 19 March 2019)

Evans (2003) 36/1 *Law Theology*
Evans M "UCITA, shrink-wrap agreements, and consumers" (2003) 36/1 *Law Theology* 1-17

Ewelukwa (2011) 13 *European Journal of Law Reform*
Ewelukwa N "Is Africa ready for electronic commerce – A critical appraisal of the legal framework for ecommerce in Africa" (2011) 13 *European Journal of Law Reform* 550-576

Faria (2004) 16 *SA Merc LJ*
Faria JE "e-Commerce and international legal harmonisation: Time to go beyond functional equivalence?" (2004) 16 *SA Merc LJ* 529-555

Fry (2001) 37/2 *Idaho Law Review*
Fry PB "Introduction to the Uniform Electronic Transactions Act: Principles, policies and provisions" (2001) 37/2 *Idaho Law Review* 237-273

Gabriel (2000) 5/4 *Uniform Law Review*
Gabriel HD "The new United States Uniform Electronic Transactions Act: Substantive provisions, drafting history and comparison to the UNCITRAL Model Law on Electronic Commerce" (2000) 5/4 Uniform Law Review 651-664

Gatt (2002) 18 *CLSR*

Gatt A "Electronic Commerce-click-wrap agreements the enforceability of click-wrap agreements" (2002) 18 *CLSR* 404-410

Giliker (2017) 37/1 *Legal Studies*
Giliker P "The consumer Rights Act 2015- A bastion of European consumer rights" (2017) 37/1 *Legal Studies* 78-102

Giliker (2015) 1 *European Review of Private Law*
Giliker P "The transposition of the Consumer Rights Directive into UK law: Implementing a maximum harmonization directive" (2015) 1 *European Review of Private Law* 5-28

Glatt (1998) 1/6 *International Journal of Law and Information Technology*
Glatt C "Comparative issues in the formation of electronic contracts" (1998) 1/6 *International Journal of Law and Information Technology* 34-64

Glushko, Tenenbaum and Meltzer (1999) 42/3 *Communications of the ACM*
Glusho R, Tenenbaum J and Meltzer B "An XML framework for agent based E-commerce" (1999) 42/3 *Communications of the ACM* 106-114

Goodman (2000) 21 *CARDOZO L REV*
Goodman B "Honey, I shrink-wrapped the consumer: The shrink-wrap agreement as an adhesion contract" (2000) 21 *CARDOZO L REV* 319-352

Goldring (1975) 6 *Federal Law Review*
Goldring J "Consumer protection and the Trade Practices Act (1974-75)" (1975) 6 *Federal Law Review* 287-339

Goldring J (1996) 2/2 *Journal of Computer Mediated Communication*
Goldring J "Consumer protection, the nation-state, law, globalization, and democracy" (1996) 2/2 *Journal of Computer Mediated Communication* 1-13

Gregory (1999) 32 *CBLJ*
Gregory JD "Solving legal issues in electronic commerce" (1999) 32 *CBLJ* 84-104

Grossman (2014) 19/4 *Berkeley Technology Law Journal*
Grossman S "Keeping unwanted donkeys and elephants out of your inbox: The case for regulating political spam" (2004) 19/4 *Berkeley Technology Law Journal* 1533-1576

Gupta (2014) 4/1 *International Journal of Computing and Corporate Research*
Gupta A "E-commerce: Role of e-commerce in today's business" (2014) 4/1 *International Journal of Computing and Corporate Research* 1-8

Hamann and Papadopoulos (2014) *De Jure*

Hamann B and Papadopoulos S "Direct marketing and spam via electronic communications: An analysis of the regulatory framework in South Africa" (2014) *De Jure* 42-62

Harland D (1991) 33/2 *Journal of the Indian Law Institute*
Harland D "Implementing the principles of the United Nations Guidelines for Consumer Protection" (1991) 33/2 *Journal of the Indian Law Institute* 189-245

Houanye and Shen (2013) 4 *Beijing Law Review*
Houanye P and Shen S "Investment protection in the framework treaty of harmonising business law in Africa (OHADA)" (2013) 4 *Beijing Law Review* 1-7

Howland (1997) 32/6 *European Transport Law*
Howland RIL "UNCITRAL Model Law on Electronic Commerce" (1997) 32/6 *European Transport Law* 703-710

Hull (2000) 51/6 *Hastings Law Journal*
Hull K "The overlooked concern with the Uniform Computer Information Transactions Act" (2000) 51/6 *Hastings Law Journal* 1391-1412

Hynick (2005) 12/1 *Southwestern Journal of Law and Trade in the Americas*
Hynick J "May I borrow your mouse? A note on electronic signatures in the United States, Argentina and Brazil" (2005) 12/1 *Southwestern Journal of Law and Trade in the Americas* 159-176

Inegbedion (2010) 2 *Justice*
Inegbedion NA "The role of regulatory agencies in respect of defective products and legal implications of certified product" (2010) 2 *Justice* 36-63

Ismail and Kamat (2006) 132 *Journal of Professional Issues in Engineering Education and Practice*
Ismail IA and Kamat VR "Evaluation of legal risk for e-commerce in construction" (2006) 132 *Journal of Professional Issues in Engineering Education and Practice* 355-360

Jacobs (2004) 16 *South African Mercantile Law Journal*
Jacobs W "The Electronic Communications and Transactions Act: Consumer protection and internet contracts" (2004) 16 *South African Mercantile Law Journal* 556-567

Jacobs, Stoop and Niekerk (2010) 13/3 *PER*
Jacobs W, Stoop P and Niekerk RV "Fundamental consumer rights under the Consumer Protection Act 68 of 2118: A critical overview and analysis" (2010) 13/3 *PER* 302-508

Jacquemin (2017) 8 *JIPITEC*

Jacquemin H "Digital content and sales or service contracts under EU law and Belgian/French law" (2017) 8 *JIPITEC* 27-38

Jarvenpaa and Todd (1997) 1 *IJEC*
Jarvenpaa SL and Todd PA "Consumer reactions to electronic shopping on the World Wide Web" (1997) 1 *IJEC* 59-88

Jenks (1953) 30 *Brit YB Intl*
Jenks CW "The conflict of law-making treaties" (1953) 30 *Brit YB Intl* 401-427

Jobodwana (2009) 4/4 *Journal of International Commercial Law and Technology*
Jobodwana ZN "E-commerce and mobile commerce in South Africa: Regulatory challenges" (2009) 4/4 *Journal of International Commercial Law and Technology* 287-298

Kajal, Saini and Grewal (2012) 2/10 *International Journal of Advanced Research in Computer Science and Software Engineering*
Kajal R, Saini D and Grewal K "Virtual private network" (2012) 2/10 *International Journal of Advanced Research in Computer Science and Software Engineering* 428-432 available at www.ijarcsse.com (date of use: 11 September 2018)

Kende (2003) 11 *Commlaw Conspectus*
Kende M "The Digital Handshake: Connecting Internet Backbones" *Commlaw Conspectus* (2003) 1 25-70

Kidd and Daughtery (2000) 26 *RCTLJ*
Kidd D Jr and Daughtery W Jr "Adapting contract law to accommodate electronic contracts" (2000) 26 *RCTLJ* 215-276

Kigerl (2009) 3/2 *International Journal of Cyber Criminology*
Kigerl AC "CAN SPAM Act: An empirical analysis" (2009) 3/2 *International Journal of Cyber Criminology* 565-589

Kightlinger (2003)24/3 *Michigan Journal of International Law*
Kightlinger MF "A solution to the Yahoo! Problem? The EC E-commerce Directive as a model for international cooperation on internet choice of law" (2003)24/3 *Michigan Journal of International Law* 719-766

Kiplagat (1995) 23/2 *Denver Journal of International Law and Policy*
Kiplagat PK "Legal status of integration treaties and the enforcement of treaty obligations: A look at the COMESA process" (1995) 23/2 *Denver Journal of International Law and Policy* 259-286

Kisielowska-Lipman (2009) *Consumer Focus*

Kisielowska-Lipman "M-pocket shopping: International consumer experiences of buying goods and services on their mobile" (2009) *Consumer Focus* 20

Koornhof (2012) 2 *Speculum Juris*
Koornhof PGJ "The enforceability of incorporated terms in electronic agreements" (2012) 2 *Speculum Juris* 41-65

Kulundu-Bitonye (1998) *Lesotho LJ*
Kulundu-Bitonye W "Electronic banking: An overview of systems and operations" (1998) *Lesotho LJ* 67- 86

Lakhani (2015) *Vindbona Journal of International Law & Arbitration*
Lakhani A "The role of transparency in the harmonization of commercial law" (2015) *Vindbona Journal of International Law & Arbitration 80 -103*

Leavitt and Whisler (1958) *Harvard Business Review*
Leavitt HJ and Whisler TL "Management in the 1980s" (1958) *Harvard Business Review* 11-21

Leng (2006) 22 *Computer Law & Security Report*
Leng TK "Electronic contracting: legal effects of input errors in e-contracting" (2006) 22 *Computer Law & Security Report* 157-164

Lilleholt (2009) 17/3 *European Review of Private Law*
Lilleholt K "Notes on the proposal for a new directive on consumer rights" (2009) 17/3 *European Review of Private Law* 335-343

Lindholm and Maennel (2000) 3 *CLR International*
Lindholm P and Maennel FA "Directive on electronic commerce (2000/31/ec)" (2000) 3 *Computer Law Review International* 16-22

Lloyd (2013) 13/7 *Without Prejudice*
Lloyd L "Signatures in the digital age: electronic Law" (2013) 13/7 *Without Prejudice* 80-82 available at www.withoutprejudice.co.za (date of use: 12 November 2019)

Lourens (1998) May *De Rebus*
Lourens J "Electronic commerce – The law and its consequences" (1998) May *De Rebus* 64-68

Malan and Pretorius (2006) 69 *THRHR*
Malan FR & Pretorius JT "Credit transfers in South African law" (2006) 69 *THRHR* 594-612

Malan and Pretorius (2007) 70 *THRHR*
Malan FR & Pretorius JT "Credit transfers in South African law" (2007) 70

THRHR 1-22

Naude (2009) 126 *SALJ*

Naude T "The consumer's right of 'fair, reasonable and just terms' under the new Consumer Protection Act in comparative perspective" (2009) 126 *SALJ* 505-536

Naude (2006) 17 *Stell LR*

Naude T "Unfair contract terms legislation: The implications of why we need it for its formulation and application" (2006) 17 *Stellenbosch LR* 361-385

Ndonga (2012) 5 *African Journal of Legal Studies*

Ndonga D "E-commerce in Africa: Challenges and solutions" (2012) 5 *African Journal of Legal Studies* 243-268

Ndubuisi, Anyanwu and Nwankwo (2016) 6/4 *Arabian Journal of Business and Management Review*

Ndubuisi E, Anyanwu A, and Nwankwo C "Protecting the Nigerian consumer: An expository examination of the role of Consumer Protection Council" (2016) 6/4 *Arabian Journal of Business and Management Review* 1-7

Niranjanamurthy et al (2013) 2/6 *International Journal of Advanced Research in Computer and Communication Engineering* 2362

Niranjanamurthy M et al "Analysis of E-commerce and m-commerce: advantages, limitations and security issues" (2013) 2/6 *International Journal of Advanced Research in Computer and Communication Engineering* 2360-2362

Ogechukwu (2013) 5/1 *International Postgraduate Business Journal*

Ogechukwu AD "Consumerism the shame of marketing in Nigeria challenges to corporate practices" (2013) 5/1 *International Postgraduate Business Journal* 1-30

Orji (2018) 12/2 *Masaryk University Journal of Law & Technology*

Orji UJ "The African Union Convention on Cybersecurity: A regional response towards cyber stability?" (2018) 12/2 *Masaryk University Journal of Law & Technology* 91-129

Orji (2018) 29/6 *International Company and Commercial Law Review*

Orji U J "Towards the Harmonisation of E-commerce Laws in West Africa: A Comparative Analysis of the ECOWAS Electronic Transactions Act" (2018) 29(6) *International Company and Commercial Law Review* 373-390

Papadopoulos (2012) 47 *THRHR*

Papadopoulos SM "Are we about to cure the scorge of spam? A commentary on current and proposed South African legislative intervention" (2012) 47 *THRHR* 223-240

Peterson, Balasubramanian and Bronnenberg (1997) 25 *JAMS*
Peterson RA, Balasubramanian S and Bronnenberg BJ "Exploring the implications of the internet for consumer marketing" (1997) 25 *JAMS* 29-46

Prosser (1960) 69 *Yale LJ*
Prosser WL "The assault upon the Citadel (Strict liability to the consumer)" (1960) 69 *Yale LJ* 1099 at 1103 as cited in Clark AM *Product Liability, Modern Legal Studies* (London: Sweet and Maxwell 1989)

Pistorius (2004) 16 *SA Merc LJ*
Pistorius T "Click-wrap and web-wrap agreements" (2004) 16 *SA Merc LJ* 568-576

Pistorius (2002) XXXV *CILSA*
Pistorius T "Contract formation: A comparative study of legislative initiatives on select aspects of electronic commerce" (2002) XXXV *CILSA* 129-156

Pistorius (1999) 11 *SA Merc LJ*
Pistorius T "Formation of internet contracts: An analysis of the contractual and security issues" (1999) 11 *SA Merc LJ* 282-299

Pistorius (1993) 5 *SA Merc LJ*
Pistorius T "The enforceability of shrink-wrap agreements in South Africa" (1993) 5 *SA Merc LJ* 1-9

Pistorius (2008) 2 *JITL*
Pistorius T "The legal effect of input errors in automated transactions: The South African matrix" (2008) 2 *JITL* 1-21

Pompian (1999) 85 *Virginia LR*
Pompian S "Is the Statute of Frauds ready for electronic contracting?" (1999) 85 *Virginia LR* 1447-1503

Quo (2004) 11/1 *Murdoch University Electronic Journal of Law*
Quo S "Spam: Private and legislative responses to unsolicited electronic mail in Australia and the United States" (2004) 11/1 *Murdoch University Electronic Journal of Law* paras 1-124

Radic (2013/2014) *European Consumer Law*
Radic L "The influence of the implementation of Art 14 of the Consumer Rights Directive in distance selling contracts on consumer protection in Spain and the United Kingdom" (2013/2014) *European Consumer Law* 1-11

Reed (2001) 36/3 *Tort & Insurance Law Journal*
Reed TS "Bond claims and the impact of the Uniform Electronic Transactions Act, the Uniform Computer Information Transactions Act, and other

Technological developments" (2001) 36/3 *Tort & Insurance Law Journal* 735-776

Robertson (2003) 78 *WLR*
Robertson M "Is assent still a prerequisite for contract formation in today's economy?" (2003) 78 *WLR* 265-296

Schulze (2006) 18 *SA Merc LJ*
Schulze C "Electronic commerce and civil jurisdiction with special reference to consumer contracts" (2006) 18 *SA Merc LJ* 31-44

Schulze (2004) 16 *SA Merc LJ*
Schulze WG "Countermanding and electronic funds transfer" (2004) 16 *SA Merc LJ* 667-684

Schulze (2004) 16 *SA Merc LJ*
Schulze WG "E-money and Electronic Fund Transfers: A shortlist of some of the unresolved issues" (2004) 16 *SA Merc LJ* 50-66

Schulze (2007) 19 *SA Merc LJ*
Schulze WG "Electronic fund transfer and the bank's right to reverse a credit transfer: One small step for banking law, one huge leap for banks" (2007) 19 *SA Merc LJ* 379-387

Schulze (2005) 17 *SA Merc LJ*
Schulze WG "Of credit cards, unauthorised withdrawals and fraudulent credit card users" (2005) 17 *SA Merc LJ* 202-213

Schurr (2007) 38 *VUWLR*
Schurr FA "The relevance of the European consumer protection law for the development of the European contract law" (2007) 38 *VUWLR* 131-144

Scupola, Hente and Nicolajsen (2009) 1/3 *International Journal of E-services & Mobile Applications*
Scupola A, Hente A and Nicolajsen H "E services: Characteristics, scope and conceptualising strengths" (2009) 1/3 *International Journal of E-services & Mobile Applications* 1-16

Seaman (2000) *Computers and Law*
Seaman A "E-commerce, jurisdiction and choice of law" (2000) *Computers and Law* 28-37

Seo (2001) 1/146 *Buffalo Intellectual Property Law Journal*
Seo C "Licenses and the Uniform Computer Information Transactions Act" (2001) 1/146 *Buffalo Intellectual Property Law Journal* 146-167

Shah (2000) 15/1 *Berkeley Technology Law Journal*
Shah PA "The Uniform Computer Information Transactions Act" (2000) 15/1 *Berkeley Technology Law Journal* 85-107

Shahjee (2016) 4/27 *SRJIS*
Shahjee R "The impact of electronic commerce on business organization" (2016) 4/27 *SRJIS* 3130-3140

Snail (2007) 15 *Juta Business Law*
Snail S "South African e-consumer law in the context of the ECT Act" (2007) 15 *Juta Business Law* 44-60.

Snail (2008) 2 *JILT*
Snail S "Electronic contracts in South Africa: A comparative analysis" (2008) 2 *JILT* 1-24

Stassen and Stassen (2002) *De Rebus*
Stassen P and Stassen K "Selected aspects of the Electronic Communications and Transactions Act" (2002) *De Rebus* 48

Stern (2001) 16 *Berkeley Technology Law Journal*
Stern JE "The Electronic Signatures in Global and National Commerce Act" (2001) 16 *Berkeley Technology Law Journal* 391-414

Stoop (2009) 21 *SA Merc LJ*
Stoop P "SMS and e-mail contracts: Jafta v Ezemvelo KZN Wildlife" (2009) 21 *SA Merc LJ* 110-125

Svantesson (2001) 17 *Computer Law & Security Reports*
Svantesson D "Jurisdictional issues in cyberspace" (2001) 17 *Computer Law & Security Reports* 318-326

Tasneem (2011) *International Journal of Management and Business Research*
Tasneem F "The legal issues of electronic contracts in Australia" (2011) *International Journal of Management and Business Research* 85-92

Tladi (2008) 125/1 *The South African Law Journal*
Tladi S "The regulation of unsolicited commercial communications (SPAM): Is the opt-out mechanism effective?" (2008) 125/1 *The South African Law Journal* (2008) 178-192

Urban, Karaganis and Schofield (2017) 64/3 *Journal of the Copyright Society of the USA*
.
Urban JM, Karaganis J and Schofield BL "Notice and takedown: Online service provider and rightholder accounts of everyday practice" (2017) 64/3 *Journal of the Copyright Society of the USA* 371-410

Uzoka, Shemi and Seleka (2017) 31/4 *Electronic Journal on Information Systems in Developing Countries*
Uzoka FE, Shemi AP and Seleka GG "Behavioural influences on e-commerce adoption in a developing country context" (2017) 31/4 *Electronic Journal on Infromation Systems in Developing Countries* 1-15

Visser (1989) 1 *SA Merc LJ*
Visser C "The evolution of electronic payment Systems" (1989) 1 *SA Merc LJ 189*-207

Visser (2003) 11/1 *Juta's Business Law*
Visser C "A new online service provider liability regime" (2003) 11/1 *Juta's Business Law* 40-44

Waller, Brady and Acosta (2011) *European Journal of Consumer Law*
Waller SW, Brady JG and Acosta RJ "Consumer protection in the United States: An overview" (2011) *European Journal of Consumer Law* 1-30

Wang (2015) 2 *Journal of Business Law*
Wang FF "The incorporation of terms into commercial contracts: a reassessment in the digital age" (2015) 2 *Journal of Business Law* 87-119

Watjatrakul (2006) 9 *AUJT*
Watjatrakul B "IT Application outsourcing: A category and evaluation of application service providers" (2006) 9 *AUJT* 209-216

Watnick (2004) *Baylor LR*
Watnick V "The electronic formation of contract and the common law 'Mailbox Rule'" (2004) *Baylor LR* 176-203

Watson (2001) 53/4 *Baylor Law Review*
Watson M "E-commerce and e-law; is everything e-okay? Analysis of the Electronic Signatures in Global and National Commerce Act" (2001) 53/4 *Baylor Law Review* 803-848

Wenninger and Laster (1995) 1/1 *Current Issues in Economics and Finance*
Wenninger J and Laster D "The electronic purse" (1995) 1/1 *Current Issues in Economics and Finance*1-7

Witte (2002) 35/2 *The John Marshall Law Review*
Witte D "Avoiding the un-real estate deal: Has the Uniform Electronic Transactions Act gone too far?" (2002) 35/2 *The John Marshall Law Review* 311-332

Zhang (2005) *Berkeley Technology Law Journal*
Zhang L "The CAN-SPAM Act: An insufficient response to the growing spam problem" (2005) 20 *Berkeley Technology Law Journal* 301-322

Zemnick (2001) 76/3 *Chicago-Kent Law Review*
Zemnick SR "The E-sign Act: The means to effectively facilitate the growth and development of e-commerce" (2001) 76/3 *Chicago-Kent Law Review* 1965-1992

Zittran (2006) 119 *Harvard Law Review*
Zittran J "The generative internet" (2006) 119 *Harvard Law Review* 1974-2040

PAPERS, REPORTS & SERIES

Amazouz "African Union perspectives on cybersecurity and cybercrime"
Amazouz S "African Union perspectives on cybersecurity and cybercrime" (Paper presented at ITU-ATU Workshop on Cybersecurity strategy in African countries, Khartoum, Sudan (Republic of the) 24-26 July 2016) 1-17

Andrade, Novais and Newes "Will and Declaration"
Andrade F, Novais P and Neves J "Will and Declaration in Acts performed by Intelligent Software Agents: Preliminary Issues on the Question" Proceedings of the 4th Workshop on the Law and Electronic Agents (LEA 2005) available at www.researchgate./publications (date of use: 24 July 2019) 1-4

Batuwa "Development and Implementation"
Batuwa SK "Development and Implementation of the EAC Regional E-Government Framework" presentation at the UN Public Administration Programme on Electronic /Mobile Government in Africa: Progress Made and Challenges Ahead 17-19 February 2009 Addis Ababa, Ethiopia 1-26

Bender *Australia's spam legislation*
Bender MR *Australia's spam legislation: A modern-day King Canute?* (2006) Corporate and Accountability Research Group Working Paper No 2 1-24

Borgen "Resolving Treaty Conflicts"
Borgen CJ "Resolving Treaty Conflicts" St John's Law Scholarship Repository (2005) Faculty Publications Paper 122 available at http://scholarship.law.stjohns.edu/faculty publications/122 (date of use 05 December 2019)

Calmet and Endsley "An Agent Framework"
Calmet J and Endsuleit RD "An Agent Framework for Legal Validation of E-Transaction" (2004) Allien Institute for Artificial Intelligence 182-184

Chirita "The impact of Directive 2011/83/EU"
Chirita AD "The impact of Directive 2011/83/EU on consumer rights" paper presented at the Ius Commune Workshop on Contract Law on 24 November 2011 in Utrecht, Netherlands 1-27

Consumer Awareness Organisation *Research report*
Consumer Awareness Organisation *Research report on the state of consumer protection in Nigeria: A review of consumer protection in the Telecommunications sector in Nigeria* (2014)

Davies "The development of laws"

Davies A "The development of laws on Electronic Documents and E-commerce Transactions" 2008 1-29 Library of Parliament (Canada) 1 available at https://publications.gc.ca (date of use: 26 August 2020)

Di Domitilla S "Court of justice"
Di Domitilla Sartorio "Court of justice: a catalyst for European integration" (2015) RISE Rivista Internazionale di studi Europei 19-23

Esselaar "What ISPs can do"
Esselaar P "What ISPs can do about Undesirable Content" (ISPA.org.za A paper Commissioned by the Internet Service Providers' Association 2008)

Gelder and Biard "Functioning of the ODR Platform"
Gelder EV and Biard A "Functioning of the ODR platform: EU Commission Publishes First Results" December 2017 (PhD & Postdoc Researchers *ERC project Building EU Civil Justice*) available at www.conflictoflaws.net (date of use: 02 July 2018)

Ha (2011) "Security and privacy"
Ha H "Security and privacy in e-consumer protection in Victoria, Australia" (2011) Springer-Verlag Berlin Heidelberg Conference paper 240-252 available at https://springer.com (date of use: 14 March 2019)

Hathaway and Savage "Duties for internet service providers"
Hathaway ME and Savage JE "Duties for internet service providers" paper presented at Munik School of Global Affairs, University of Toronto, March 2012 1-24

Hermann "Establishing a legal framework for electronic commerce"
Hermann G "Establishing a Legal Framework for Electronic Commerce: The work of the United Nations Commission on International Trade (UNCITRAL)" (1999) Paper presented at WIPO International Conference on "Electronic Commerce and Intellectual Property" 14th-16th September 1999, Geneva 2

Ibam, Boyinbode and Afolabi (2017) *EAI Endorsed Transactions on Serious Games* 4/15
Ibam EO, Boyinbode OK and Afolabi MO (2017) *EAI Endorsed Transactions on Serious Games* 4/15 "e-Commerce in Africa: the case of Nigeria" 1-6

International Trade Center "International e-commerce in Africa"
International Trade Center "International e-commerce in Africa: The way forward" (2015) 1-47 (technical paper of the ITC by WTO & UN)

Lodder "Electronic Contract and Signatures"
Lodder A "Electronic Contract and Signatures: National Civil Law in the EU will change drastically soon" 2000 Paper Presented at the 15th BILETA Conference

on "Electronic Datasets and Access to Legal Information" 14 April 2000, University of Warwick, England

Manko "Contracts for supply of digital content"
Manko R "Contracts for supply of digital content: a legal analysis of the Commission's proposal for a new directive" European Parliamentary Research Service (2016) 1-36

McNamara and O'Shea "Minimising legal risks in electronic contracting"
McNamara J and O'Shea K (2007) "Minimising legal risks in electronic contracting" in Proceedings Collector (Collaborative Electronic Commerce Technology and Research) Conference, Melbourne

Okoli and Mbarika "A framework for accessing e-commerce in Sub-Saharan Africa"
Okoli C and Mbarika V "A framework for accessing e-commerce in Sub-Saharan Africa" (2003) 1-31 (paper submitted for publication to the *Journal of Global Information Technology Management*)

Onuoha "The state of internet access and infrastructure in Nigeria"
Onuoha R "The state of internet access and infrastructure in Nigeria" (Paper presented at the Nigerian internet school of governance Lagos, Nigeria 2019) 1-16

Pessi "Exploring mobile e-commerce" 2
Pessi K "Exploring mobile e-commerce in geographical bound retailing" (2001) (conference paper February 2001) published in Research Gate 1-10

Pistorius and Hurter "Contracting on the internet"
Pistorius T and Hurter E "Contracting on the internet: The formation of contracts, trade practices and online dispute resolution" Academic paper commissioned by the Department of Communications for: "Green Paper on Electronic Commerce for South Africa" 2000 1-21

Reagle Eskimo Snow & Scottish Rain: Schema Design
Reagle J "Eskimo Snow & Scottish Rain: Legal considerations of schema design" 1999 Berkman Centre Working Draft https://cyber.harvard.edu le 1999 1-27 available at www.w3.org/tr/1999/note (date of use: 28 June 2019)

Ross "Empowering e-consumers"
Ross P "Empowering e-consumers: Strengthening consumer protection in the internet economy" Conference paper at Conference on empowering e consumers, Washington 9 December 2009 available at pdf www.oecd.org/econsumerconference (date of use: 20 October 2019)

Snail and Matanzima (2011) *Without Prejudice*.

Snail S and Matanzima S "Electronic wills – beyond the *Macdonald v the Master* decision" (2011) *Without Prejudice* 61-62

Stuber *The electronic purse*

Stuber G *The electronic purse*. An overview of recent developments and policy issues (1996) A report on use of smart cards in Canada by Stuber, Staff, Bank of Canada 1-74

Tarasewich, Nickerson and Warkentin "Wireless/Mobile E-commerce"

Tarasewich P, Nickerson RC and Warkentin M "Wireless/Mobile E-commerce: Technologies, applications, and issues" (2001) Seventh Americas Conference on Information Systems 435-438 available at www.paws.kettering.edu (date of use: 20 August 2019)

Verbiest *et al Study on the Liability of Internet Intermediaries*

Verbiest T *Study on the Liability of Internet Intermediaries* EU Commission (MARKT/2006/09/E) 2007

Verhaeghe and Woolfrey "Understanding COMESA and the East African power pool"

Verhaeghe E and Woolfrey S "Understanding COMESA and the East African power pool: Incentive-based institutional reform?" 2017 Paper prepared for the European Center for Development Policy Management (ECDPM) 1-13

Vesterdorf "Proceedings of the Court"

Vesterdorf B "Proceedings of the Court of first instance in 2003" available at https://curia.europa.eu/jcms/pdf (date of use: 05 July 2019)

Vogler, Moschgath and Kunkelmann "Enhancing mobile agents"

Vogler H, Moschgath M, and Kunkelmann T "Enhancing mobile agents with electronic commerce capabilities" (1998) International Workshop on Cooperative Information Agents 148-159

Vonken "Balancing processes in international family law"

Vonken APMJ "Balancing processes in international family law, on the determination and weighing of interests in the conflict of laws and the 'openness' of the choice of law system" Forty years on: The evolution of postwar private international law in Europe: Symposium in celebration of the 40th anniversary of the Centre of Foreign Law Private International Law, University of Amsterdam 27 October, 1989 171-194 available at www.worldcat.org (date of use: 28 June 2018)

Wright "Electronic contracting"

Wright C "Electronic contracting in an insecure world" (2008) GIAC Legal Issues 1-37

CASE LAW

AUSTRIA
Content Services Ltd v Bundesarbeitskammer (2012) Case C-49/11

AUSTRALIA
Dow Jones & Company Inc v Gutnick (2002) HCA 56 (210 CLR 575), 77 ALJR 255; 194 ALR 433

CANADA
Paccar Financial Itee v Kingsway, General Insurance Company 2012 QCCA 1030 (can LII) available at http://www.Canlii.org (date of use: 22 September 2020)

EUROPEAN UNION
Administrazione delle finanze dello Stato v Simmenthal SpA (1978) ECR 629
Francovich v Italy Case C- 6/90 ECLI: EU:C:1991:428
*The Queen v Secretary of State for Transport, Ex parte: Factortame Ltd and o*thers Case C-213/89) ECR 1990 1-02433
Van Gend en Loos v Netherlandse Administratie der Belastingen Case 26/62 1963 ECR 1, 1970 CMLR 1)

GERMANY
Bundesverband der Verbraucherzentralen und Verbraucherverbande – Ver braucherzentrale Bundesverband eV (Federal Union) v Deutsche Apotheker- und Arztebank eG (*DAAB*) C-380/19

NIGERIA
Anene v Airtel (unreported) FCT/HC/CV/545/2015
Babatunde v Bank of the North Ltd & Ors (2012) vol 206 LRCN 70
Barewa Pharmaceuticals Limited v FRN (unreported) Suit No SC.530/2016 judgment delivered on 12 April 2019
Dr Imoro Kubor v Hon Seriake Henry Dickson (2014) 4 NWLR (Part 1345) 534
Elizabeth Anyaebosi v RT Briscoe (1987) 3 NWLR (Part 59) 84
Manya v Idris (2000) FWLR (Pt 23) 1237
MTN Nig Ltd v Anene (2018) LPELR 44447 (CA)
OB Nigeria PLC v OBC Ltd (2005) 123 LRCN 191
Ogundepo v Olumesan (2012) 203 LRCN 163
Thor Ltd v FCMB (2005) 6 SC 9

SOUTH AFRICA
Africa Solar v Divwatt 2002 (4) SA 681 (SCA)
Bok Clothing Manufacturers (Pty) Ltd v Lady Land Ltd 1982 (2) SA 565 (C)
Bush and Others v BJ Kruger Incorporated and another (2013) 2 All SA 148 (GSJ)
Collen v Reitfontein Engineering Works 1948 (1) SA 413 (A)
Dlovo v Brian Porter Motors 1994 (2) SA 518 (C)
Driftwood Properties (Pty) Ltd v McLean 1971 (3) SA 591 (A)

Estate Breet v Peri-Urban Areas Health Board 1955 (3) SA 523 (A)
George v Fairmead (Pty) Ltd 1958 (2) SA 465 (A)
Gincrete (Pty) Ltd v Scherringhuisen Construction (Pty) Ltd 1996 (2) SA 682 (N)
Jafta v Ezemvelo KZN Wildlife (2008) 10 BLLR 954 (LC)
Kergeulen Sealing and Whaling Co Ltd v CIR 1939 AD 487
Ketler Investments CC t/a Ketler Presentations v Internet Service Providers' Association (2014) 1 All SA 566 (GSJ)
King's Car Hire (Pty) Ltd v Wakeling 1970 (4) SA 640 (N)
Macdonald & others v The Master & others 2002 (3) SA 64 (N)
Nissan South Africa (Pty) Ltd v Marnitz NO and others (Stand 186 Aeroport (pty) Ltd Intervening) (2006) 4 All SA 120 (SCA), 2005 (1) SA 441 (SCA)
Reid Brothers (SA) Ltd v Fischer Bearings Co Ltd 1943 AD 232
Richman v Ben-Tovim 2007 (2) SA 283 (SCA)
Sihlali v South African Broadcasting Corporation Ltd (J700108) (2010) ZALC 1; (2010) 31 ILJ 1477 (L)
Sonap Petroleum (SA) (Pty) Ltd v Papadogianis 1992 (3) SA 234 (A)
Spring Forest Trading 599 CC v Willberry (Pty) Ltd t/a Ecowash and Another 2015 (2) SA 118 (SCA)
Watermeyer v Murray 1911 AD 61

SPAIN
Travel Vac SL v Manuel Jose Antelm Case C-423/97, (1999) ECR 1-2195

UNITED KINGDOM
Brinkibon Ltd v Stahag Stahl und Stahlwarenhandelgesellschaft mbH (1982) 1 All ER 293
Entores Ltd v Miles Far Eastern Corp (1995) 2 QB 326
Godfrey v Demon Internet Ltd (1999) QBD 26
Grant v Google (2006) All ER (D) 243 (May)
Schroder Music Publishing Co Ltd v Macauley (1974) 3 All ER 616
Sir Elton John & Ors v Countess Joulebine (2001) MCLR 91
Totalise PLC v Motley Fool Ltd (2001) All ER (D) 290 (Dec)
Tournier v National Provincial Bank (1924) 1KB 461
WS Tankship II BV v The Kwangju Bank Ltd and another (2011) EWHC 3103 available at www.bailii.org/ew/cases/EWHC (date of use: 22 September 2017)

UNITED STATES OF AMERICA
America Library Association v Pataki 969 F Supp 160 (SDNY {1997})
Application Group Inc v Hunter Group Inc 61 (App 4th 881, 72)
Barnes v Yahoo! Inc Case 05-36189 (9th Cir Jun 22 2009)
Benincasa v Dentalkit Case C-269/95 (1997) ECR 1-3767
Religious Technology Centre v Netcom On-line.Comm 907 F Supp 1361-Dist Court (ND California 1995)
Binder v Aetna Life Ins Co Cal App 4th 832, 850. 89 Cal Rptr 2d 540. 551 (Cal Ct App 1999)

Brower V Gateway 2000 Inc 676 NYS 2d 569 (NYAD 1998)
Calder v Jones 465 US 783 (1984)
Carafano v Metrosplash.com 339 F 3d 1119 (9th Cir 2003)
Clipp Designs v Tag Bags 1996 F Supp 766 (ND 111 1998)
Digital Control v Boretronics 161 F Supp 2d 1186 (WD Wash 2001)
Evolution Online Systems Inc v Koninklijke Nederland NV 145 F 3d 505 (2nd Cir 1998)
Fair Housing Council of San Fernando Valley v Roommates.com LLC 521 F 3d 1157 (9th Cir 2008)
Firth v State of New York 775 NE 2d 463 (NY 2002)
Goddard v Google Inc 640 F Supp 2d 1193 (ND Cal Jul 30 2009)
Gruber v BayWa AG Case C-464/01 (2005) ECR 1-439
Inset System v Instruction Set 937 F Supp 161 (D Conn 1996)
Intel Corp v Integraph 195 F 3d 1346 (Fed Cir 1999)
International Shoe Co v Washington 326 US 310, 316 (1945)
MA Mortenson Co v Timberline Software Corporation 998 P 2d 305 (Wash Supreme Court 2000)
Medtronic Inc v Janess 729 F 2d 1395 (11th Cir 1984)
Metcalf v Lawson 802 A 2d 1221 (NH 2002)
Mieczkowski v Masco Corp 997 F Supp 782 (ED Texas 1998)
Millennium Enterprises V Millennium Music 33 F Supp 2d 907, 1999 US Dist 49
Mzarro v Home Depot Inc 544 F 3d 1230 CA 11 Circuit 2008
Parma Tile Mosaic & Marble Co v Estate of Fred Short & C, MLRS Construction Corp 87 NY 2d 524, 663 NE 2d 63 (NY 1966)
People Solutions Inc v People Solutions Inc NO CIV A 339-CV 2339-L 2000 WL 1030619 (ND Tex 2000)
Pollstar v Gigmania Ltd 170 F Supp 2d 974 (Dist Court ED California 2000)
ProCD Inc v Zeidenberg 86 F 3d 1447 (Court of Appeal 7th Circuit 1996)
Registrar.Com Inc v Verio Inc 126 F Supp 2d 238 (Dist Court SD New York 2000)
Religious Technology Center v Netcom On-line Communications Services, Inc 907 F. Supp. 1361 (US Dist Court California 1995)
Schnabel v Trilegiant Corp 697 F.3d 110 (2d cir 2012) 112ff
Sega Enterprises Ltd v MAPHIA 857 F Supp 679, 683 (ND Cal 1994)
Shute v Carnival Cruise Lines 113 Wash 2d 763, 771 (P 2d 78 1989)
Sidney Blumenthal and Jacqueline & Anor v Matt Drudge and America Online Inc CIV A 97-1968 PLF 1998
Specht v Netscape Comms Corp 306 F 3d 17 - Court of Appeals 2nd Circuit 2002
Ticket Master Corporation v Tickets.Com Inc NOCV 99-7654, 2000 WL 525390 (CD Cal 27 March 2000)
Winfield Collection v McCauley 105 F Supp 2d 746 (ED MICH 2000)
Zippo Manufacturing Co v Zippo Dot Com 952 F Supp 1119 (WD Pa 1997)
Google Scholar.com available at www.googlescholar/caselaw (date of use: 16 November 2018)

LEGISLATION & STATUTORY INSTRUMENTS

AUSTRALIA
ACTS
Competition and Consumer Act, 2010
Electronic Transactions Act 162 of 1999 (amended by Electronics Transactions Amendment Act, 2011)
Federal Privacy Act, 1988
Spam Act 2003
REGULATIONS
Electronic Transactions Regulations, 2000

NIGERIA
ACTS
Constitution of the Federal Republic of Nigeria, 1999 (amended 2011)
Consumer Protection Council Act, Cap C25 LFN 2004
Cybercrime (Prohibition, Prevention, Etc) Act, 2015
Electronic Transactions Bill, 2017
Evidence Act 18 of 2011
Federal Competition and Consumer Protection Act, 2019
Interpretation Act LFN 2004
National Agency for Food and Drug Administration and Control Act Laws Federation of Nigeria (LFN) Cap N7 2004
National Information Technology Development Agency Act, 2007
Nigeria Communications Act, 2015
Sale of Goods Law (Cap 150) Laws of Bendel State, 1976
Standards Organisation of Nigeria Act Cap S9 LFN 2004
Supreme Court Ordinance, 1876
Supreme Court Ordinance, 1914
Supreme Court Proclamation, 1900
Trade Malpractices (Miscellaneous Offences) Decree, 1992
REGULATIONS
Data Protection Regulations 2019
Nigeria Communications Commission (Registration of Telephone Subscribers) Regulations, 2011
NITDA Public Key Infrastructure Regulations 2014

SOUTH AFRICA
ACTS
Consumer Protection Act 68 of 2008
Electronic Communications and Transactions Act 25 of 2002
Enforcement of Foreign Civil Judgments Act 32 of 1988
Protection of Personal Information Act 4 of 2013
UNITED KINGDOM
ACTS

Consumer Rights Act, 2015
Data Protection Act, 1998
Electronic Communications Act 2000 Ch0700
REGULATIONS
Consumer Contracts (information, cancellation and additional charges) Regulations 2013 No 3134
Consumer Protection from Unfair Trading Regulations 2008 No 1277
Consumer Protection (Amendment) Regulations 2014 No 870
Consumer Rights (Payment Surchages) Regulations 2012 No 3110
Electronic Commerce (EC Directive) Regulations 2002 No 2013
Payment Services Regulation 2017 No 752
Regulation (EC) No 2006/2004 on Consumer Protection Cooperation
Unfair Terms in Consumer Contracts Regulation 1999 No 2083

UNITED STATES OF AMERICA
ACTS
Controlling the Assault of Non-Solicited Pornography and Marketing Act 2003
Communications Decency Act, 1996
Do-Not-Call Implementation Act 15 USC Ch 87A 2003
Electronic Communications Privacy Act Amendment Act, 2015 amending the Electronic Communications Privacy Act, 18 USC 1986
Electronic Signatures in Global and National Conference Act, 2000
Equal Credit Opportunity Act 15 USC s 1974
Federal Trade Commission Act 15 USC 1999
Restore Online Shopper's Confidence Act 15 USC ch 110 s8401 2010
Uniform Computer Information Transactions Act 2002
Uniform Electronic Transactions Act 2009
Uniform Electronic Will Act 2019

CONVENTIONS AND STATUTORY INSTRUMENTS

REGIONAL

AFRICAN UNION
African Union Convention on the Establishment of a Legal Framework Conducive to Cyber Security in Africa 2012 (AU Convention)

COMMON MARKET FOR EASTERN AND SOUTHERN AFRICA
Model Law on Electronic Commerce (COMESA Model Law) 2010

COMMONWEALTH OF NATIONS
(Draft) Commonwealth Model on Electronic Transaction (2002)

EAST AFRICAN COMMUNITY

East African Community Treaty 1999
Framework for Cyberlaws Phase I (EAC Framework I) 2008
Draft Framework for Cyber Laws Phase II February 2011

ECOWAS

ECOWAS Supplementary Act A/SA 1/01/07 on the Harmonisation of Policies and of the Regulatory Framework for the Information and Communications Technology (ICT) Sector, 2007
ECOWAS Supplementary Protocol A/SP.1/06/06 amending the revised treaty of 1 June 2006
Supplementary Act A/SA.2/01/10 on Electronic Transactions in the ECOWAS Area adopted at the 37th Session of the Authority of Heads of State and Government Abuja, 16 February 2010

EUROPEAN UNION

Council Regulation (EC) No 44/2001 of 22 December 2000 on Jurisdiction and the Recognition and Enforcement of Judgements in Civil and Commercial Matters *OJL* 12, 16.1.2001, 1-23 (Brussels Convention)
Directive 93/13/EEC on Unfair Terms in Consumer Contracts *OJL* 95, 21.4.1993 29-34
Directive 95/46/EC of the European Parliament and the Council of October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of such Data
Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 Concerning the Processing of Personal Data and the Protection of Privacy in the Telecommunications Sector
Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures
Directive 2000/31/EC of the European Union and of the Council of 8 June 2000 on Certain Legal Aspects of Information Society Services in Particular Electronic Commerce in the Internal Market (E-commerce Directive) *OJL* 178, 17.7.2000 1-16
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 Communication Sector which is soon to be repealed by the proposed Regulation on the respect for private life and the protection of personal data in electronic communications (ePrivacy Regulation)
Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 Concerning Unfair Business-to-Consumer Commercial Practices in the Internal Market *OJL* 149,11.6.2005 22-39
Directive 2006/123/EC of the European Parliament and of the Council of 12 December 2006 on Services in the Internal Market *OJL* 376, 27.12.2006, 36-68
Directive 2007/64/EC of the European Parliament and of the Council of 13 November 2007 on Payment Services in the Internal Market

Directive 2009/110/EC of the European Parliament and of the Council of 16 September 2009 on the taking up, pursuit and prudential supervision of the business of electronic money institutions *OJL* 267,10.10.2009
Directive 2011/83/EU of the Parliament and of the Council of 25 October 2011 on Consumer Rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council Text with EEA relevance *OJL*, 304, 22.11.2011 64-88
Directive 2013/11/EU of the European Parliament and of the Council of 21 May 2013 on Alternative Dispute Resolution for Consumer Disputes and Amending Regulation (EC) No 2006/2004 and Directive 2009/22/EC *OJL* 165,18.6.2013 63-79
Directive (EU) 2019/2161 of the European Parliament and of the Council of 27 November 2019 amending Council Directive 93/13/EEC and Directives 98/6/EC, 2005/29/EC and 2011/83/EU of the European Parliament and of the Council as Regards the Better Enforcement and Modernisation of Union Consumer Protection Rules *OJL* 328, 18.12.2019 p 7-28
European Communities Act of 1972
European Union Treaty 1992 (also known as the Maastricht Treaty)
European Union (Withdrawal) Act 2018
Regulation (EC) 593/2008 of the European Parliament and of the Council of 17 June 2008 on the law applicable to contractual obligations *OJL* 177, 4.7.2008 6-16
Regulation (EU) No 1215/2012 of the European Parliament of 12 December 2012 on Jurisdiction and the Recognition and Enforcement of Judgements in Civil and Commercial Matters (Brussels Regulation) OJL 351, 20.12.2012 1-32
Regulation (EU) No 524/2013 of the European Parliament and of the Council of 21 May 2013 on Online Dispute Resolution for Consumer Disputes and amending Regulation (EC) No 2006/2004 and Directive 2009/22/EC
Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with regard to the Processing of Personal Data and on the Free Movement of such Data (this Regulation repeals Directive 95/46/EC of the European Parliament)
Regulation (EU) 2017/2394 of the European Parliament and of the Council of 12 December 2017 on Cooperation Between National Authorities Responsible for the Enforcement of Consumer Protection Laws and Repealing Regulation (EC) 2006/2004 by 16 January 2020 *OJL* 345, 27.12.2017 1-26
Regulation (EU) 2018/302 of the European Parliament and of the Council of 28 February 2018 on addressing unjustified geo-blocking and other forms of discrimination based on customers' nationality, place of residence or place of establishment within the internal market and amending Regulations (EC) No 2006/2004 and (EU) 2017/2394 and Directive 2009/22/EC *OJL* 601, 2.3.2018, 1-15

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT

Consumer Dispute Resolution and Redress Recommendation 2007
Convention on the Organisation for Economic Co-operation and Development, Paris 14th December 1960

Recommendation of the OECD Council concerning Guidelines for Consumer Protection in the Context of Electronic Commerce 1999
Recommendation of the Council Concerning Guidelines for Protecting Consumers from Fraudulent and Deceptive Commercial Practices across Borders 2003
OECD (2016) Consumer Protection in E-Commerce: OECD Recommendation, OECD Publishing

ORGANISATION FOR THE HARMONISATION OF BUSINESS LAW IN AFRICA

Treaty on the Harmonisation of Business Law in Africa (OHADA Treaty) revised 2008
Uniform Act Relating to General Commercial Law 2014

SOUTHERN AFRICAN DEVELOPMENT COMMUNITY

Southern African Development Community Model law on Electronic Transactions and Electronic Commerce adopted in Mauritius November, 2012, by SADC Ministers responsible for Telecommunications, Postal and ICT
Southern African Development Community Model law on Data Protection 2012

INTERNATIONAL

HAGUE CONFERENCE ON PRIVATE INTERNATIONAL LAW

The Hague Convention on the Law Applicable to Contracts for the International Sale of Goods 1986

UNITED NATIONS

UNCITRAL Model Law on Electronic Commerce 1996
UNCITRAL Model Law on Electronic Signatures (2001)
UNCITRAL Model Law on Electronic Transferable Record adopted 13 July 2017
United Nations Convention on Contracts for the International Sale of Goods 1980 (Vienna Convention)
United Nations Convention on the use of Electronic Communications in International Contracts (Res 60/21 2005) Publication Sales No E.07.v.2.
United Nations International Covenant on Economic, Social and Cultural Rights 1966
United Nations Universal Declaration of Human Rights 10 December 1948

OFFICIAL REPORTS

NATIONAL REPORTS

AUSTRALIA

The Australian Guidelines for Electronic Commerce 2006

NIGERIA

Central Bank of Nigeria Guidelines on Electronic Banking in Nigeria, 2003
Central Bank of Nigeria Guide to Bank Charges, 2004
Data Interoperability Standards 2016

Framework and Guidelines for the Use of Social Media Platforms in Public Institutions 2019
Guidelines for Clearance of Information Technology (IT) Projects by Public Institutions 2018
Guidelines for Nigeria Content Development in Information and Communications Technology (ICT) 2013
Guidelines for Registration of ICT Service Providers/Contractors for Delivery of IT Services to MDAs 2018
National Information Systems and Network Security Standards and Guidelines 2013

SOUTH AFRICA

Department of Communications "Green Paper on Electronic Commerce for South Africa-for public discussion" (2000) Executive Summary, Chapters 2 & 3 available at pdf https://www.westerncape.gov.za/text (date of use: 28 June 2018)
Department of Trade and Industry *Consumer Affairs Committee Annual Report 2008/2009* available at https://www.gov.za (date of use: 19 October 2020)
Draft Southern African Development Community Model Law on Electronic Transactions and Electronic Commerce, 2012

UNITED KINGDOM

DTI *A Guide for Business to the Electronic Commerce (EC Directive) Regulations 2002* (2002) available at www.out-law.com (date of use: 16 October 2020)
Office of Fair Trading *Internet Shopping An OFT market study* (2007)

UNITED STATES

US Department of Commerce Economic Statistics Administration, office of Policy Development *The emerging digital economy II* (June 1999)

INTERNATIONAL ORGANISATIONS

EUROPEAN UNION

Booys TQ & Hesselink MW "EU contract law" (Paper, Center for the study of European Contract Law 2009) 1-45
Commission of the European Communities "Consumer Behaviour in the Internal Market" July 1991
European Commission, DG Internal Market and Services Unit Study on the Economic Impact of the Electronic Commerce Directive Final Report 7 September 2007
European Commission "Payment Card Chargeback When Paying over the Internet" Report of sub group meeting of the PSTDG & PSULG July 2000
European Commission "Report from the Commission to the European Parliament and the Council on the Application of Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on Consumer Rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and Repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council" 23 May 2017
European Parliament *Towards new rules on sales and digital content: Analysis of the key issues* (2017)

European Union *The Proposal for a Directive on Consumer Rights: Impact on Level of National Consumer Protection. Comparative Table* 2009
Glossary of the terms related to quality assurance from the Tempus Joint European Project for the Development of Quality Assurance
Loos MGM "The influence of European Consumer law on general contract law and the need for spontaneous harmonisation" (Paper, Center for the study of European Contract Law No 2006/02) 1-34
Muller *et al Consumer behaviour in a digital environment* (European Parliament 2011)
Nielsen CK *et al Study of the Economic Impact of the Electronic Commerce Directive* (DG Internal Market and Service, European Commission 2007)

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT

OECD *Better regulation in Europe: United Kingdom* (2010)
OECD *Consumer education policy recommendations of the OECD's Committee on consumer policy* (2009)
OECD "Consumer policy guidance on intangible digital content products"
(OECD Digital Economy Papers No 241 2014) 1-22
OECD "Consumer policy guidance on mobile and online payments" (OECD Digital Economy Papers, No 236 2016) 1-23
OECD *Consumer protection enforcement in a global digital marketplace* (OECD Digital Economy Papers No 266) 2018
OECD "Empowering e-consumers: Strengthening consumer protection in the internet economy" Washington, DC 8-10 December 2009
(OECD) Guidelines on the Protection of Individuals with Regard to the Processing of Personal Data (1981)
OECD "Improving online disclosures with behavioural insights" (STI policy note 2018) 1-8
OECD *Online advertising trends, benefits and risks for consumers* (OECD Publishing 2019)
OECD "Online product safety sweeps results" (OECD Digital Economy Papers No 262 2016) 1-44
OECD *Proposed Clarification of the Permanent Establishment Definition 2004*
(2006 Anti-Spam Toolkit)
OECD "Protecting consumers in peer platform markets exploring the issues" (OECD Digital Economy Papers No 253 2016) 1-31
OECD *Report on the implementation of the 2003 OECD Guidelines for protecting consumers from fraudulent and deceptive commercial practices across borders* (2006)
OECD *Strengthening consumer protection in the internet economy* (Background report of the OECD Conference on empowering e-consumer Washington DC 8-10 December 2009)
OECD *Toolkit for protecting digital consumers* (2018)
OECD "Working Party on the Information Economy Report DSTI/ ICCP/IE (2004) 18/FINAL of 18 April 2006"
2007 Mobile Commerce Guidance

2008 OECD Policy Guidance for Addressing Emerging Consumer Protection and Empowerment Issues in Mobile Commerce
2008 Online Identity Theft Guidance
2014 Digital Content Product Guidelines
2014 Mobile and Online Payments Guidelines

UNITED NATIONS

Faria J A "Model laws as tools for legal harmonisation: The experience of UNCITRAL" (UNCITRAL report) 1-21
General Assembly Resolution 70/1 of 27 June 2016 of the Human Rights Council on the Promotion, Protection and Enjoyment of Human Rights on the Internet
ITU *HIPSSA-ICT regulatory harmonisation: A comparative study of regional initiatives* 2009
OHCHR General Assembly res 70/1 of June 2016 of the Human Rights Council res A/HRC/32/L.20 on the Promotion, Protection and Enjoyment of Human Rights on the Internet available at www.ohchr.org (date of use: 22 June 2018)
UN *Legal aspects of automatic data processing: note by the Secretariat* 1983 A/CN.9/238
UN "Technical Notes on Online Dispute Resolution of the United Nations Commission on International Trade Law" available at htpp://odr.info/un-general-assembly-resolution-on-odr (date of use: 22 February 2019)
UNCITRAL Possible future work on Online Dispute Resolution in Cross-border Electronic Commerce transactions (43rd Session 26 May 2010)
UNCITRAL "Status: United Nations Convention on the use of Electronic Communications in International Contracts" (New York, 2005) available at www.uncitral.org (date of use: 28 June 2019)
UNCITRAL Technical Notes on Online Dispute Resolution adopted by the UN General Assembly on the 13 December 2016 (unpublished)
UNCITRAL Working Group IV (Electronic Commerce) Legal Issues Relating to the Use of Electronic Transferable Records 46th Session (2012)
UNCITRAL Promoting Confidence in Electronic Commerce: Legal Issues on International Use of Electronic Authentication and Signature Methods (2009)
UNCTAD "Consumer protection in e-commerce" (2017) (Note by UNCTAD secretariat) 1-17
UNCTAD Expert Meeting on Cyberlaws and Regulations for Enhancing E-commerce, Including Case Studies and Lessons Learned 25 - 27 March 2015, Geneva, Switzerland available at www.ecowas.int/ecowas-law (Date of use: 14 March 2019)
UNCTAD *Harmonising cyberlaws and Regulations: The experience of the East African Community* 2013
UNCTAD *Review of E-commerce legislation harmonization in the Economic Community of West African States (*United Nations, 2015)
United Nations Guidelines for Consumer Protection 2015 first adopted in 1985, expanded in 1999 and revised and adopted by the General Assembly in resolution 70/186 of 22 December 2015 available at https://unctad.org (date of use: 19 March 2019)

NON GOVERNMENTAL ORGANISATIONS
COPENHEN ECONOMICS
Jervelund C "Study on the Economic impact of the E-commerce Directive" (2008) 1-9

ACADEMY OF THE EUROPEAN LAW FORUM
Howells G and Reich N "The current limits of European harmonisation in consumer contract law" (Paper of the Academy of European Law Forum 2011) 39-57

INSTITUTE FOR SECURITY STUDIES
Tamakin E "The AU's cybercrime response" (2015 Policy brief 73) 1-8

KENYA ICT ACTION NETWORK
Githaiga A report of the online debate on African Union Convention on Cybersecurity (AUCC) 2013 1-23

WEB SOURCES

Abyssinialaw "The organs of African Union" available at https://abyssinialaw.com (date of use: 28 October 2020)

ADMA "About ADMA" available at www.adma.com.au (date of use: 14 October 2020)

Adobe "US guide to electronic signatures. An overview of federal and state law" 2017 https://acrobat.adobe.com (date of use: 30 October 2020) 1-4

African Peer Review Mechanism *The African Governance Report* (2019) 26 available at www.au.int (date of use: 19 July 2020)

AG "Australia Plans to accede to the EC Convention" available at http://www.ag.gov.au (date of use: 04 September 2019)

Agbajileke O "Senate Reconsiders Passes Federal Competition and Consumer Protection Bill" available at www.businessdayonline.com/05 December 2018 (date of use 05 October 2020)

Aldrich M "Internet online shopping" available at www.aldricharchive.com/internet_shopping.html (date of use: 12 July 2020)

Alkali R "West Africa: ECOWAS-Its Formation and Achievements" AllAfrica 2008 available at www.allafrica.com (date of use: 22 August 2020)

Alperin J et al "BBN A Case History of Transition" (2001) 43 available at www.web.mit.edu (date of use: 17 August 2020)

Amta "Lost and stolen phones" available at www.amta.org.au (date of use: 06 October 2020)

Anritsu *Wireless Technology Terms Glossary and Dictionary* available at www.anritsu.com (date of use: 18 August 2020)

Antovski L and Gusev M "Mobile commerce services" 2003 available at www.researchgate.net/publications (date of use: 09 February 2019) 15-24

Aphref.com "The payment system-overview" 23-36 available at www.aph.gov.au (date of use: 14 February 2019)

ARB "Welcome to the Advertising Regulatory Board" available at www.arb.org.za (date of use: 20 June 2020)

ARIN "IP Addresses and Domain Names" available at www.arin.net (date of use: 18 August 2020)

AU "African Union Convention Cyber Security and Personal Data Protection" available at https://au.int (date of use: 26 June 2020)

AU "AU in a Nutshell" available at www.au.int/en (date of use: 13 October 2020)

AU "List of countries which have signed, ratified/acceded to the African Union
Convention on Cyber Security and Personal Data Protection" available at http://au.int (date of use: 20 October 2020)

AU "Member state profiles" available at https://au.int/en/treaties (date of use: 08 October 2020)

AU "Southern African Development Community (SADC)" available at www.au.int (date of use: 26 July 2020)

Australian Government "Australia - European Union Free Trade Agreement" available at www.dfat.gov.au (date of use: 06 October 2020)

Australian Government "How Government works" available at www.australia.gov.au/about-government (date of use: 13 October 2020)

Australian Government "United Nations Convention on the Use of Electronic Communications in International Contracts" available at www.australia.gov.au (date of use: 04 October 2020)

Barrons *Dictionary of Marketing Terms* available at www.allbusiness.co/barrons dictionary (date of use: 18 August 2020)

BBC News "Article 50: UK set to formally trigger Brexit process" 29 March 2017 available at www.bbc.com (date of use: 16 October 2020)

BBC News "Nigeria telecom giant MTN fined a record 5.2bn" 26 October 2015 available at https://www.bbc.com/news (date of use: 22 October 2020)

BBC "UK no longer a member of EU" 31 January 2020 available at www.bbc.co.uk (date of use: 25 May 2020)

Bourgeois D and Bourgeois DT *Information Systems and Beyond* (Chapter Five) available at https://bus 206.pressbooks.com (date of use: 17 August 2020)

Carnegie Mellon School of Computer Science "The ISPs Role of Improving Internet Security" available at www.cs.cmu.edu (date of use: 22 September 2020)

Cetinyilmaz E"New regulation on distance contracts" (2015) available at www.erdem-erdem.av.tr (date of use: 20 January 2019)

CIO "Credit and investment ombudsman" available at http://www.cio.org.au (date of use: 13 October 2020)

Clarke O "Why US agreement terms don't always work in Europe" available at pdf www.osbourneclarke.com (date of use: 14 February 2019)

Clarke R "Electronic commerce definitions" Roger Clarke available at www.rogerclarke.com (date of use: 02 July 2020)

Cloete E (2003) "SME's in South Africa: Acceptance and Adoption of e-Commerce" 1-12 available at www.researchgate.net (date of use: 16 August 2020)

Collins Dictionary "Definition of 'inertia selling'" available at www.collinsdictionary.com (date of use: 25 October 2020)

Collins Dictionary "Definition of SMS" available at www.collinsdictionary.com (date of use: 22 February 2019)

COMESA "Member States" available at https://comesa.int (date of use: 26 June 2020)

COMESA *COMESA in brief* available at https://www.comesa.int/pdf (date of use: 26 July 2020)

COMESA "Overview of COMESA" available at http://comesa.int (date of use: 26 August 2020)

CommonwealthDraft Commonwealth Model Law available at www.thecommonwealth-ilibrary.org (date of use: 30 January 2019)
Communications Alliance "Overview" available at www.commsalliance.com.au (date of use: 14 October 2020)
Consumer finance "Consumer Sentinel Network Data Book" available at https://www.consumerfinancemonitor.com (date of use: 04 October 2020)
Consumers International "About Consumers International and our members" available at https://consumersinternational.org (date of use: 20 October 2020)
Cupido R "Offer and acceptance in cross-border electronic contracts: A brief comparative perspective" 2015 1-9 available at www.ase-scoop.org (date of use: 05 September 2020)
Definitions.net "What does e-services mean?" available at www.definitions.net (date of use: 20 June 2020)
Dictionary.com "Local Area Network (LAN)" available at www.dictionary.com (date of use: 03 March 2020)
DMASA *Code of ethics and standards of practice* available at https://www.outprosysys.com/dmadmasa.org (date of use: 20 June 2020)
EAC "Overview of EAC-East African Community" available at www.eac.int (date of use: 26 June 2020)
ECOWAS "Member states" available at www.ecowas.int (date of use: 22 August 2020)
ECOWAS "Official Journal – Supplementary Acts/Protocols/Decisions/New Regime for Community Acts" available at www.ecowas.int/ecowas-law (date of use: 14 August 2020).
Educaloi "Rights and responsibilities of service providers in contracts for services" available at https://www.educaloi.qc.ca (date of use: 16 October 2020)
Efxkits "Wireless Communication Technologies Types and Advantages" available at www.efxkits.us (date of use: 18 August 2018)
Emsisoft Diagram of "effect of spam" available at https://blog.emsisoft.com (date of use: 20 July 2019)
Emsisoft Diagram "How a Botnet works" available at https://blog.emsisoft.com (date of use: 20 July 2020)
Erdle M "On-line Contracts: Electronic Creation of Effective Contracts" 2001 Deeth Williams Wall available at www.dww.com/articles/online (date of use: 08 August 2020)
ECOWAS "Official Journal – Supplementary Acts/Protocols/Decisions/ New Regime for Community Acts" available at www.ecowas.int/ecowas-law (date of use: 14 January 2020)
Ellet J "New research shows growing impact on online research on in-store purchases" (2018) available at https://www.forbes.com (date of use: 03 October 2020)
Ellipsis "Electronic Communications and Transactions Amendment Bill" available at www.ellipsis.co.za (date of use: 05 September 2020)
European Consumer Centers/Network *Chargeback in the EU/EEA* (A solution to get

your money back when a trader does not respect your consumer rights) 17 available at https://ec.europakonsument.at pdf (date of use: 18 September 2020)

EU "Antitrust: Commission fines Google €1.49 billion for abusive practices in online advertising" 20 March 2019 available at https://www.ec.europa.eu (date of use: 25 November 2019)

EU "Consumer Protection Cooperation Network" available at https://ec.europa.eu (date of use: 28 July 2020)

EU "Member states" available at https://europa.eu (date of use: 21 July 2020)

EU "EU Treaties" available at https://europa.eu (date of use: 16 May 2020)

EU "European Union regulations" available at www.eur-lex.europa (date of use: 25 October 2020)

EU "How the European Union works" available at https//:www.europarliamentti.info.en (date of use: 25 October 2020)

EU "Precedence of European Law" available at www.eur.europa.eu (date of use: 05 June 2020)

EU "Regulations, Directives and other Acts" available at https://europa.eu/eu-law/legal-acts (date of use: 16 October 2020)

EU "Role of the ECC-NET" available at www.europa.eu (date of use: 02 October 2020)

EU "The history of the European Union" available at http://europa.eu/about (date of use: 21 July 2020)

EU "The institution" available at https://curia.europa.eu (date of use: 03 October 2020)

Europa "Court of justice of the European Union (CJEU)" available at https:///www.europa.eu (date of use: 28 October 2020)

Europarl "The court of justice of the European Union" available at https://www.europarl.europe.eu (date of use: 28 October 2020)

European Payment Institutions Federation "Merchant acquiring" available at https://paymentinstitutions.eu (date of use: 14 October 2020)

Faria J "Legal Harmonisation through model laws: The experience of the United Nations Commission on international trade law (UNCITRAL)" 1-8 available at www.justice.gov.za (25 November 2019)

Financial Dictionary "Virtual Mall" available at https://financial-dictionary.thefreedictionary.com (date of use: 20 June 2020)

Firstdata.com *First Data Payments Industry Glossary* (2012) available at https://www.firstdata.com (date of use: 14 October 2020)

Flechtner H "United Nations Convention on Contracts for the International Sale of Goods Vienna, 11 April 1980" available at www.legal.un.org (date of use: 10 October 2020)

Freshdirect.com "Potato order account" available at https://www.freshdirect.com (date of use: 10 October 2020)

Frost & Sullivan "Desktop virtualisation: Implementing the workplace of the future, to

day" 2015 available at www.fujitsu.com (date of use: 18 August 2020)

FTC "Cell phones and the Do Not Call Registry" available at www.consumer.ftc.gov (date of use: 28 October 2020)

FTC "Consumer Sentinel Network" available at https://www.ftc.gov (date of use: 28 October 2020)

FTC "Enforcement" available at https://ftc.gov>enforcement (date of use: 15 July 2020)

Garners R "Early Popular Computers, 1950-1970" available at www.ethw.org (date of use: 17 August 2020)

Government SA "Structure and Functions of the South African Government" available at www.gov.za/about-government (date of use: 20 September 2020)

Gov.UK "EU legislation and UK law" available at www.legislation.gov.uk (date of use: 16 May 2020)

GTAD "Meeting of the East African Community (EAC) Task Force on Cyber laws" available at www.gtad.wto.org (date of use: 30 November 2020)

Ha H "'Three-sector governance system' Model to address fives issues of consumer protection in B2C e-commerce in Victoria, Australia" 1-15 available at www.anzam.org (date of use 14 October 2020)

Haentjens O "Shopping Agents and their Legal implications regarding Austrian Law" (2011) available at www.citeseerx.ist.psu.edu 1-14 (date of use: 28 June 2020)

HCCH "41: Convention of 2 July 2019 on the Recognition and Enforcement of Foreign Judgements in Civil and Commercial Matters" available at https://www.hcch.net (date of use: 16 October 2020)

HCCH "Electronic commerce and the internet" (Press release 26 June 2003) available at https://www.hcch.net (date of use: 20 October 2020)

HCCH "More about HCCH" available at https://www.hcchh.net/en/home (date of use: 09 October 2020)

HCCH "Members and parties" available at https://www.hcch.net (date of use: 20 October 2020)

Hccourt *Dow Jones & Company Inc v Gutnick* available at http://eresources.hccourt.gov.au (date of use: 13 June 2019)

History.com *History of the UN* available at www.history.com/topics (date of use: 28 August 2020)

History.com "Invention of the PC" available at https://www.history.com (date of use: 22 February 2019)

History.com "Sputnik launched" available at www.history.com (date of use: 30 July 2020)

Howstuffworks.com "How did the internet start?" available at https://computer.howstuffworks.com (date of use: 30 July 2020)

IBM *Dictionary of IBM & Computing Terminology* available at https://www-03.ibm>pdf (date of use: 20 October 2019)

ICC "Dispute resolution" available at https://iccwbo.org (date of use: 20 October 2020)

IJRC "Court of Justice of the European Union" available at https://ijrcenter.org (date of use: 18 October 2020)
Information Regulator – Department of Justice available at www.justice.gov.za (date of use: 24 November 2019)
Internetguide "ARPA/DARPA: Contribution to the creation of the internet" available at www.internet-guide.co.uk (date of use: 26 July 2020)
Intertek "Information for importers" available at www.exports2nigeria.com (date of use: 23 October 2020)
Internetlivestat "Internet users in the world" www.internetlivestats.com (date of use: 16 June 2018)
Internetworldstats "Internet penetration in Africa" available at www.internetworldstats.com (date of use: 09 September 2018)
Internetworldstats "World internet usage and population statistics –updated" available at www.internetworldstats.com (date of use: 20 November 2020)
Internetworldstats "Internet world statistics" available at www.internetworldstats.com (date of use: 27 November 2020)
Kobrin S "Economic governance in an electronically networked global economy" available at www.faculty.wharton.upenn.edu (date of use: 18 October 2020)
Konga "Return policy" available at www.konga.com (date of use: 05 July 2020)
Konrad "ZI Konrad Zuse internet archive" available at http://.zuse.zib.de (date of use: 24 May 2019)
Kotz D & Gray RS "Mobile agents and the future of the internet" Department of Computer Science/Thayer School of Engineering Dartmouth College, Hannover, New Hampshire 1999 available at http://www.cs.dartmouth.edu (date of use: 21 August 2020)
Lawaspect.com "Uniform Computer Information Transactions Act (UCITA)" available at https://lawaspect.com (date of use: 24 October 2020)
Lawteacher *Brinkibon Ltd v Stahag Stahl und Stahlwarenhandelgesellschaft mbH* available at http://www.lawteacher.net/cases (date of use: 15 October 2020)
Legal Aid Society Northeasthern NY "The differences between Federal, State, and Local Laws" available at https://www.lawhelp.org (date of use: 30 October 2020)
Lifewire.com "Understanding Wi-Fi and how it works" available at www.lifewire.com (date of use: 07 February 2020)
Marius "Wireless application service provider" available at https://mybroadband.co.za (date of use: 10 October 2020)
Worldwide.com "The size of the World Wide Web (The internet)" available at www.worldwidewebsize.com (date of use: 16 December 2020)
MEAC "Common market" available at https://meac.go.ke (05 July 2020)
Michalsons "The law vs unsolicited commercial communications" 2003 www.michalsons.com (date of use: 30 December 2020)

Moore FO "Routers" (2017) 1-10 available at https://www.researchgate.net/publication/317057644 (date of use: 18 August 2020)

NASS "Acts of the National Assembly" available at https://www.nass.gov.ng (date of use: 20 June 2020)

NASS "Votes and proceedings" available at https://www.nass.gov.ng (date of use: 20 June 2020)

National Capital Legal Services "Consumer Protection" available at m.ncls-inc.com/consumerrights (date of use: 15 February 2019)

NCC "Internet users in Nigeria hit 98.3 million" December 2018 available at www.ncc.gov.ng/thecommunicator/index (date of use: 15 October 2020)

NCC "Welcome" available at www.thencc.gov.za (date of use: 15 October 2020)

Niescier T ed "Virtual courts and the future of personal jurisdiction" (2012) available at https://www.jurist.org (date of use: 20 October 2020)

NITDA "Background" available at http://nitda.gov.ng (date of use: 15 October 2020)

NITDA "Standards & Guidelines" available at https://www.nitda.gov.ng (date of use: 10 October 2020)

North Carolina Judicial Branch "Business Court Technology" available at https://www.nccourts.gov (date of use: 20 October 2020)

NSF "About NSFNET" available at www.nsfnet-legacy.org (date of use: 29 May 2019)

OECD "About the OECD" available at www.oecd.org/about (date of use: 16 October 2020)

OECD "European Union and the OECD" available at www.oecd.org (date of use: 20 November 2020)

OECD "Partnerships in OECD bodies" available at www.oecd.org (date of use: 03 July 2020)

OECD "South Africa and the OECD" available at www.oecd.org (date of use: 15 October 2020)

OECD "Where: Global reach" available at www.oecd.org (date of use: 05 September 2020)

OHADA "General overview" available at https://www.ohada.org (date of use: 09 September 2020)

OHADA "History of OHADA" available at https://www.ohada.org (date of use: 15 October 2020)

Onifade A "History of the Computer" 7 available at www.ethw.org/pdf (date of use: 16 August 2020)

Parliament of Australia "Electronic Transactions Amendment Bill 2011" available at https://www.aph.gov.au (date of use: 16 October 2020)

Peter I "So who really did invent the internet?" available at www.nethistory.info (date of use: 13 August 2020)

Pinsent Masons "Online dispute resolution platform now operational" 18 February 2016 available at www.pinsentmasons.com (date of use: 18 October 2020)

Pinterest Diagram of 'Wan' available at https://www.pinterest.ca (date of use: 03 July 2019)
Pizza Hut "Pizza Hut celebrates 20th anniversary of world's first online purchase with 50 percent off online deal for Hut lovers members" available at https://prnewswire.com (date of use: 02 September 2020)
PLACNG "E-transactions Bill passes third reading" available at http://placng.org (date of use: 25 October 2020)
PLACNG "Senate passes Federal Competition and Consumer Protection Bill" 08 June 2017 available at https://www.placng.org (date of use: 02 October 2020)
PLACNG "State of Consumer Protection Bill in Nigeria" available at https://placng.org/home (date of use: 06 December 2019)
Pomp U (MMS) "Konzept und Implementierung eines Shopping-Agenten-Systems fur elektronische Marktplatze" available at http://www.medienassistent.org (date of use: 16 September 2020)
Pratt M (2013) "How fast is a T1 internet line and what is it?" available at https://www.business.org (date of use: 19 August 2020)
Pulse "President Buhari has rejected a bill seeking to protect the right of internet users in Nigeria from infringement" 21 March 2019 available at https://www.pulse.ng (date of use: 02 July 2020)
Punch "Konga extends pay on delivery to Abuja" 12 February 2019 available at https://punchng.com/konga (date of use: 05 October 2020)
PWC "Demystifying the merchant acquiring business" (2018) available at https://www.pwc.in (date of use: 14 February 2019)
Rouse M "Point-of-Presence" available at www.searchnetworking.techtarget.com (date of use: 07 October 2020)
Rushton C "The History of Amazon.com" available at https://www.techwala.com (date of use: 03 August 2020)
Government SA "Structure and Functions of the South African Government" available at www.gov.za/about-government (date of use: 20 September 2019)
Samme-Nlar T "Why it is important for African States to ratify the Malabo Convention" available at https://www.aanoip.org (date of use: 29 October 2020)
SADC "About SADC" available at www.sadc.int (date of use: 20 October 2020)
SADC "Tripartite cooperation" available at www.sadc.int (date of use: 26 August 2020)

SBA "Office of the National Ombudsman" available at https://www.sba.gov (date of use: 28 October 2020)
Saleh K "Global online retail spending – statistics and trends" available at www.invespcro.com (date of use: 03 October 2020)
Searchsecurity "Distibuted denial of service (DDoS) attack" available at http://searchsecurity.techtarget.com (date of use: 20 September 2020)
Searchsecurity "What is botnet?" available at http://searchsecurity.techtarget.com (date of use: 20 September 2020)
Simplynotes "Origin of electronic commerce/history of e-commerce and evolution of e-commerce" available at www.simplynotes.in (date of use: 20 June 2020)

Small Business Administration "Regulatory fairness" available at https://www.sba.gov (date of use: 28 June 2019)
Strickland J "Who owns the internet?" available at https://computer.howstuffworks.com (date of use: 18 August 2020)
Study.com "What is the Uniform Law Commission?" available at https://study.com (date of use: 30 November 2020)
Supremecourt "Role of the Supreme Court" available at http://www.supremecourt.uk (date of use: 01 October 2020)
Techopedia "What is a T1 line? available at https://www.techopedia.com (date of use: 29 May 2020)
Techopedia "What is a Botnet herder?" available at www.techopedia.com (date of use: 20 September 2020)
Techterms *The Tech Terms Computer Dictionary* available at http://techterms.com (date of use: 13 August 2020)
Techterms "EDI" available at www.techterms.com (date of use: 15 October 2020)
Techviews.com "Top Nigerian Mobile Network Operators" available at www.techviews.com.ng (07 October 2020)
Telephone Preference Service "Welcome" available at https://www.tpsonline.org.uk (date of use: 20 October 2020)
Thompson Reuters "Uniform Electronic Transactions Act (UETA)" available at https://content.next.westlaw.com (date of use: 19 June 2020)
The Guardian"ECOWAS moves to harmonise cyberlaws for e-commerce" 06 April 2015 available at https://guardian.ng/ecowas (date of use: 26 June 2020)
The Law Dictionary "What is service contract?" available at http://thelawdictionary.org (date of use: 20 June 2020)
Tyson J "How internet infrastructure works" 2001 available at http://computer.howstuffworks.com (date of use: 26 August 2020)
UCITA Online "The Uniform Computer Information Transactions Act (UCITA) is a pro posed state contract law" available at www.ucitaonline.com (date of use: 24 October 2020)
UKECC "What is the UK European Consumer Center" available at http://www.ukecc.net (date of use: 07 October 2020)
ULC "Electronic Will" available at https://www.uniformlaws.org (date of use: 19 July 2020)
ULC *FAQ – How does an act receive final UCL approval?* available at https://www.uniformlaws.org (date of use: 01 July 2020)
UN "Member states" available at https://www.un.org (date of use: 25 November 2020)
UN "Status: United Nations Convention on the use of Electronic Communications in International Contracts (New York, 2005) available at www.uncitral.un.org (date of use: 21 January 2021).
UNCITRAL "UNCITRAL Model Law on Electronic Commerce (1996) – status" available at www.uncitral.org (date of use: 28 October 2020)
UNCITRAL United Nations Convention on the use of Electronic Communications in international contracts" available at www.uncitral.org (date of use: 28 October 2020)

UNCITRAL United Nations Convention on the use of Electronic Communications in international contracts 'status'" available at www.uncitral.org (date of use: 11 October 2020)

UNCTAD "Cyber Legislation in the Economic Community of West African States (ECOWAS) Region" available at www.unctad.org (date of use: 05 October 2020)

UNCTAD "Data protection and privacy legislation worldwide" available at www.unctad.org (date of use: 06 June 2021)

UNCTAD "E-transactions legislation worldwide" available at https://unctad.org (date of use: 30 November 2020)

UNCTAD "Summary of adoption of e-commerce legislation worldwide" available at www.unctad.org (date of use: 03 July 2020)

UNCTAD "East African Community" available at http://unctad.org (date of use: 05 July 2020)

UNECA "Regional economic communities" available at http://www.uneca.org/oria (date of use: 13 October 2020)

UNECA COMESA "Common Market for Eastern and Southern Market" available at www.unec.org (date of use: 30 November 2020)

USA Government "How the US government is organized" available at https://usa.gov (date of use: 15 July 2020)

Vanguard News "Buhari assents to Federal Competition, Consumer Protection Act 2019" 07 February 2019 available at www.vanguardngr.com (date of use: 07 October 2020)

Viscasillas S "Michigan creates cyber court" (2002) available at https://cio.com (date of use: 15 October 2020)

Waxman OB "eBay 20th Anniversary: First item Sold" available at www.time.com (date of use: 02 October 2020)

WASPA "About WASPA" available at www.waspa.org.za (date of use: 20 June 2019

Webster *New World Telecom Dictionary Online-Your Dictionary* available at www.yourdictionary.com (date of use: 18 August 2020)

WhatIsMyIPAddress.com "Without IP Addresses, the internet would disappear" available at www.whatismyipaddress.com (date of use: 06 October 2020)

Wilmerhale "The origin of click-wrap: software shrink-wrap agreements" (2000) available at www.wilmerhale.com (date of use: 14 October 2020)

Wouters P "The History of information technology – Spine theme demo" (2017) available at www.spine.paulwp.com (date of use: 18 October 2020)

WTO "Electronic commerce" (2017) available at www.wto.or/english/thewto_e/ecom (date of use: 20 June 2020)

INDEX