THE REGULATION OF UNSOLICITED ELECTRONIC COMMUNICATIONS (SPAM) IN SOUTH AFRICA: A COMPARATIVE STUDY

by

SEBOLAWE ERNA MOKOWADI TLADI

submitted in accordance with the requirements
for the degree of

DOCTOR OF LAWS

at the

UNIVERSITY OF SOUTH AFRICA

SUPERVISOR: PROF T PISTORIUS

JUNE 2017

DECLARATION

I, **Sebolawe Erna Mokowadi Tladi**, (33675813) declare that **THE REGULATION OF UNSOLICITED ELECTRONIC COMMUNICATIONS (SPAM) IN SOUTH AFRICA: A COMPARATIVE STUDY** is my own work and that all the sources I have used or quoted have been indicated and acknowledged by means of complete references.

I declare further that this thesis or any part of it has not been submitted to another university or any other organisation for any other purpose.

…………………………   …………………………
Signature   Date
Sebolawe E.M. Tladi

SUMMARY

The practice of spamming (sending unsolicited electronic communications) has been dubbed "the scourge of the 21st century" affecting different stakeholders. This practice is also credited for not only disrupting electronic communications but also, it overloads electronic systems and creates unnecessary costs for those affected than the ones responsible for sending such communications. In trying to address this issue nations have implemented anti-spam laws to combat the scourge. South Africa not lagging behind, has put in place anti-spam provisions to deal with the scourge. The anti-spam provisions are scattered in pieces of legislation dealing with diverse issues including: consumer protection; direct marketing; credit laws; and electronic transactions and communications. In addition to these provisions, an Amendment Bill to one of these laws and two Bills covering cybercrimes and cyber-security issues have been published.

In this thesis, a question is asked on whether the current fragmented anti-spam provisions are adequate in protecting consumers. Whether the overlaps between these pieces of legislation are competent to deal with the ever increasing threats on electronic communications at large. Finally, the question as to whether a multi-faceted approach, which includes a Model Law on spam would be a suitable starting point setting out requirements for the sending of unsolicited electronic communications can be sufficient in protecting consumers. And as spam is not only a national but also a global problem, South Africa needs to look at the option of entering into mutual agreements with other countries and organisations in order to combat spam at a global level.

KEY WORDS

Anti-spam laws; commercial electronic messages; consumers; consent; direct marketing; dictionary attacks; disguising of headers (spoofing); electronic communications; electronic mail (e-mail); harvesting and sale of e-mail addresses; international cooperation; opt-out mechanism; opt-in mechanism; personal information; spam; unsolicited bulk email; unsolicited commercial communications; unsolicited electronic communications.

TABLE OF ABBREVIATIONS

ABN	Australian Business Number
ACA	Australian Communications Authority
ACMA	Australia Communications and Media Authority
ACN	Australian Company Number
ADMA	Australian Direct Marketing Association
ADV	Advertisement
ADV: ADLT	Advertisement: Adult
AISI	Australian Internet Security Initiative
AMU	Arab Maghreb Union
AOL	America Online
APCAUCE	Asia-Pacific Coalition against Unsolicited Commercial e-mail
APWG	Anti-phishing Working Group
ARAPKE	African Regional Action Plan for the Knowledge Economy
ARPA	Advanced Research Project Agency
ARPAnet	Advanced Research Projects Agency Networks
APEC	Asia Pacific Economic Cooperation
ASEAN	Association of Southeast Asia Nations
ASA	Advertising Standards' Authority of South Africa
ATU	African Telecommunication Union
AU	African Union
AUCC	African Union Convention on Cybersecurity
CAFTEC	*Conference des administrations des postes et des telecommunications d'expression Francaise*

CAN-SPAM	Controlling the Assault of Non-Solicited Pornography and Marketing Act
CASL	Canada Anti-Spam Legislation
CAUBE	Coalition against Unsolicited Bulk Commercial E-mail
CAUCE	Coalition against Unsolicited Commercial e-mail
CEM	Commercial Electronic Message
CEN-SAD	Community of Sahel-Saharan States
CERT	Computer Emergency Response Team
COMESA	Common Market of Eastern and Southern Africa
CFR	Code of Federal Regulation
CPA	Consumer Protection Act
CPC	Consumer Protection Council (Nigeria)
CSIRT	Computer Security Incidence Response Team
CTSS	Compatible Time Sharing Systems
DBL	Domain Block List
DEC	Digital Equipment Corporation
DMA	Direct Marketing Association
DMASA	Direct Marketing Association of South Africa
DNS	Domain Name System
DPA	Data Protection Authority
EAC	Eastern African Community
ECCAS	Economic Community of Central African States
ECT ACT	Electronic Communications and Transactions Act
E-COMMERCE	Electronic Commerce
ECOWAS	Economic Community of West African States
ECSP	Electronic Communications Service Providers
EDI	Electronic Data Interchange
E-FILING	Electronic Filing

EFCC	Economic and Financial Crimes Commission
E-MAIL	Electronic Mail
EMS	Emailing Message Service
E-PETITIONS	Electronic Petitions
E-TRANSACTIONS	Electronic Transactions
ESPS	Email Service Providers
EU	European Union
FTC	Federal Trade Commission
FTP	File Transfer Protocol
gTLD	Generic Top Level Domain
GSR	Global Symposium for Regulators
HGH	Human Growth Hormone
HIPCAR	Harmonization of ICT Policies in the Caribbean
HIPSSA	Harmonization of ICT Policies in Sub-Saharan Africa
HTML	Hypertext Mark-up Language
HTTP	Hypertext Transfer Protocol
IASP	Internet Access Service Provider
ICB4PAC	Harmonization of ICT Policies in the Pacific Island Countries
ICANN	Internet Corporation for Assigned Names & Numbers
*i*CAUCE	International Coalition against Commercial E-mail
ICT	Information and Communications Technology
ID	Identity
IGAD	Intergovernmental Authority for Development
IGADD	Intergovernmental Authority on Drought and Development
IAS	Internet Access Service

IASP	Internet Access Service Provider
IIA	Internet Industry Association
IoT	Internet of Things
IMP	Interface Message Processor
IP	Internet Protocol
IRB	Industry Representative Body
IRC	Internet Relay Chat
ISOC	Internet Society
ISP	Internet Service Provider
ISPA	Internet Service Provider Association
ITU	International Telecommunications Union
ITU-D	(ITU) Telecommunication Development
ITU-R	(ITU) Radio-communications
ITU-T	(ITU) Telecommunication Standards
ITU-T X	International Telecommunications Union T Series X
IVR	Interactive Voice Response
LAP	London Action Plan
LSG	Lead Study group
MAAWG	Messaging Anti-abuse Working Group
MCEMA	Maryland Commercial E-mail Act
M-COMMERCE	Mobile Commerce
MMA	Mobile Marketing Association
MMS	Multimedia Messaging Service
MoU	Memorandum of Understanding
NCA	National Credit Act
NCC	National Consumer Commission
NOIE	National Office Information Economy (Australia)

NRA	National Regulatory Authority
OAU	Organisation of the African Unity
OECD	Organisation for Economic Cooperation and Development
PBL	Policy Block list
PC	Personal Computer
POPI ACT	Protection of Personal Information Act
POP-UP-ADS	Pop up Advertisements
PROFECO	*Procuraduria Federal Del Consumidor*
PTA	Preferential Trade Area for Eastern and Southern Africa
RECs	Regional Communities
ROSKO	Register of Known Spam Operations
SA	South Africa
SADC	Southern African Development Cooperation
SADCC	Southern African Development Coordination Conference
SAHO	South African History Online
SARS	South African Revenue Service
SBL	Spamhaus Block List
SG 17	Study Group 17
SIM	Subscriber Identity Module
SMS	Short Message Service
SPF	Sender Policy Framework
SPIM	Instant Messaging Spam
TSAG	Telecommunication Standardization Advisory Group
UBCE	Unsolicited Bulk Commercial E-mail

UBE	Unsolicited Bulk E-mail
UBEM	Unsolicited Bulk Electronic Message
UCC	Unsolicited Commercial Communications
UCE	Unsolicited Commercial Electronic Mail
UCEA	Unsolicited Commercial E-mail Advertisement
UCEM	Unsolicited Commercial Electronic Message
UEM	Unsolicited Electronic Mail
UK	United Kingdom
UN	United Nations
UNCITRAL	United Nations Commission on International Trade Law
UNCTAD	United Nations Conference on Trade and Development
UNECA	United Nations Economic Commission for Africa
UNECIC	United Nations Convention on the use of Electronic Communications in International Contracts
USA	United States of America
USC	United States Code
USENET	User’s Network
UT	University of Texas
VoIP	Voice over Internet Protocol
WSIS	World Summit on Information Society
WSIS+10	World Summit on Information Society: United Nations Assembly General Meeting High level
WTSA	World Telecommunication Standardization Assembly
WWW	World-wide web
XBL	Exploits block list

ACKNOWLEDGEMENTS

A project of this magnitude requires that credit be given where it is due. I would therefore like to thank Prof Pistorius, my promoter, for the guidance and support provided in the writing process, and also Prof Neville Botha and Dr Nwabueze for the valuable input during the editing process. A word of thanks is extended to my colleagues and friends in the department of Mercantile Law, the College of law and UNISA at large for cheering me on.

Most importantly, my gratitude goes out to my family for not only believing in me and inspiring me to be the best but also for the sacrifices made throughout this journey. Thanks to my husband Dire Tladi for believing in me and encouraging me to move on even when giving up seemed like an option. One of the many valuable lessons I've learned from you is: "to finish what I've started", which encouraged me to go on no matter the obstacles. Thanks also for partnering with me in raising the two gifts that this life has bestowed upon us. To our light (Lesedi) and our victory (Ofentse) thank you for taking care of your stomachs (lol) while I was working on the "encyclopedia". You remain my greatest inspiration in this lifetime. My joy is seeing you two living your lives with purpose and resolve and excelling at using the talents you've been entrusted with. You are the future.

To the village that raised me and nurtured me, thank you for the sacrifice and continued support. To my mother Dorcas Lemekoana (a.k.a Dekokos), thanks for being the pillar of strength not only to me but to my siblings: my late sister Mantsha (whom we miss dearly); Kwena; Phetolo; and Kujo. You have singlehandedly shaped our tender spirits and today as we navigate adulthood and parenthood we remain people of character. Thank you for always telling us: "if you fall, you must have the sense to stand up, dust yourself off and move on". Those words of wisdom are still a compass to this day. You continue to love beyond measure and in your "bonus years" you enjoy the fruits of our motherhood (our heritage your grandchildren). To my favourite nephews and nieces you are the best.

To the extended family members and friends who've contributed to my life's journey: the late Malome Mmirwa Malekane for stimulating my curious mind and challenging me to reach for greater heights; Malome Jeka waga Lemekoana, for telling me "whatever happens I must not despair" a golden nugget that still carries me to this day; Abuti Mateu Ramagoshi, for being a sounding board and providing guidance and support; baga Mabitsela; my in-laws, baga Molopyane; and baga Tladi (also remembering my late mother-in-law the original "Mma Tladi" Eva Tladi, a woman of noble character.

To the older women (my mothers') and sisters in the four corners of this world who've mentored and prayed me through thank you.

To the ancestors who've transitioned, you live in us and we live to see you again. We will continue to meditate on your words of wisdom and in all our doings we will strife to:

"Know ourselves".

TABLE OF CONTENT

DECLARATION I

SUMMARY II

KEY WORDS III

TABLE OF ABBREVIATIONS IV

ACKNOWLEDGEMENTS X

CHAPTER 1 1

BACKGROUND TO THE STUDY 1

1.1 Introduction 1

1.2 Scope and purpose of this study 5

1.2.1 Title 5

1.2.2 Study objectives 5

1.2.3 Research question 5

1.2.4 Hypothesis 6

1.2.5 Rationale of the thesis 6

1.2.6 Parameters 6

1.3 Synopsis: Chapter trajectory 8

CHAPTER 2 12

DIRECT MARKETING AND THE DEVELOPMENT OF SPAM VIA ELECTRONIC COMMUNICATIONS 12

2.1 Introduction 12

2.2 Direct marketing 13

2.2.1 Traditional marketing versus electronic marketing 14

2.2.1.1 Background 14

2.2.1.2 Comparison between traditional marketing and electronic marketing 15

2.3 Development of spam via electronic communications 17

2.3.1 Background 17

2.3.2 The evolution of spam via electronic communication 18

2.3.2.1 ARPAnet and the first signs of junk mail (spam) 18

2.3.2.2 Types of spam message in an electronic environment 20

2.4 Lucrative business for spammers 33

2.5 Conclusion 35

CHAPTER 3 37

THE EFFECT OF SPAM ON E-MAIL MESSAGES 37

3.1 Introduction 37

3.2 Methods used to extract e-mail addresses for purposes of spam 37

3.2.1 Background 37

3.2.2. Online profiling and the use of cookies 38

3.2.2.1 Online profiling 38

3.2.2.2 Cookies 40

3.2.3 Harvesting e-mail addresses 41

3.2.4 Dictionary attacks 43

3.2.5 Spyware 44

3.2.6 Spoofing (disguising headers) 46

3.3 Problems caused by spam 46

3.3 1 No costs to the sender but to the recipients and ISPs 46

3.3.2 Flooding of recipients' mailboxes 48

3.3.3 Wasting time reading and discarding unwanted messages 48

3.3.4 Fraudulent practices and objectionable content 49

3.3.5 Stifling of communication 49

3.4 Technical measures for combating spam 50

3.4.1 Background 50

3.4.2 Types of technical measures in place to combat spam 50

3.4.2.1 Filters 50

3.4.2.2 Blocking spam by using blacklists and whitelists 53

3.4.2.3 Spam fighters 54

3.5 Conclusion 55

CHAPTER 4 57

INTERNATIONAL INITIATIVES TO COMBAT SPAM 57

4.1 Introduction 57

4.2 International Telecommunications Union (ITU) 57

4.2.1 Background.. 57

4.2.2 The Telecommunication Standards Sector (ITU-T) 59

4.2.2.1 Introduction... 59

4.2.2.2 Study Group 17 60

4.3 Countering and combating spam 60

4.3.1 Background.. 60

4.3.2 Survey conducted 62

4.3.3 Approaches to combating spam by the ITU 63

4.3.4 A comprehensive or multi-pronged approach to combatting spam (Resolution 52) 64

4.3.4.1 Background 64

4.3.4.2 Strong legislation 64

4.3.4.3 Development of technical tools and best practices 81

4.3.4.4 The establishment of industry partnership 84

4.3.4.5 Consumer education 85

4.3.4.6 International cooperation 86

4.3.5 Conclusion 87

4.4 The OECD 89

4.4.1 Background.. 89

4.4.2 The OECD’s initiatives in combating spam 89

4.4.2.1 Task Force on spam 89

4.4.2.2 The Anti-spam Toolkit 90

4.4.2.3 Eight elements contained in the Anti-spam Toolkit 91

4.4.3. Conclusion 103

4.5 Commentary and conclusion on the ITU and OECD initiatives 104

CHAPTER 5 107

REGIONAL INITIATIVES TO COMBAT SPAM: AFRICAN REGION 107

5.1 Introduction 107

5.2 African Region 107

5.2.1 Background 107

5.2.2. African Union 108

5.2.3 Regional integration in the African region 109

5.2.3.1 COMESA 111

5.2.3.2 SADC 112

5.2.3.3 ATU 112

5.3 Combating spam in the African region 113

5.3.1 Introduction 113

5.3.2 African Union 114

5.3.2.1 Background 114

5.3.2.2. African Union Convention on Cyber Security and Personal Data Protection 115

5.3.3 COMESA Model Law on Electronic Transactions and Guide to Enactment 124

5.3.3.1 Background 124

5.3.3.2 Consumer protection 125

5.3.3.3 Combating spam under the COMESA Model Law ... 126

5.3.4 SADC ... 129

5.3.4.1 Harmonisation of ICT Policies in sub-Saharan Africa ... 129

5.3.4.2 SADC Model Law ... 130

5.3.5 ATU ... 135

5.3.5.1 Cooperation between ATU and other stakeholders ... 135

5.4 Contexualisation of the African region’s Model Laws and Conventions ... 137

5.4.1 Uniformity among instruments: definitions ... 137

5.4.2 Contrasting the instruments: mechanisms ... 138

5.4.3 Requirements in regulating electronic communications ... 138

5.5 Conclusion ... 139

CHAPTER 6 ... 141

A COMPARATIVE STUDY OF ANTI-SPAM LAWS: THE UNITED STATES OF AMERICA (USA) ... 141

6.1 Introduction ... 141

6.2 Anti-spam laws at state level in the USA ... 141

6.2.1 Background ... 141

6.2.2 Features of anti-spam laws at state level ... 142

6.2.2.1 Definition of spam in state laws ... 142

6.2.2.2 Mechanisms to regulate spam ... 148

6.2.2.3 Labelling of e-mail messages ... 151

6.2.2.4 Falsified or misleading headers and information ... 152

6.2.2.5 Harvesting and sale of lists and the use of dictionary attacks ... 156

6.2.2.6 Enforcement and penalties ... 157

6.2.2.7 Commentary and conclusion ... 158

6.3 Anti-spam legislation at federal level ... 160

6.3.1 Background 160
6.3.2 Anti-spam provisions under CAN-SPAM Act of 2003 161
6.3.2.1 Definitions 161
6.3.2.2 Mechanism to regulate spam: Opt-out mechanism 162
6.3.2.3 Requirements for transmission of e-mail messages 164
6.3.2.4 Enforcement of the Act 173
6.3.2.5 Other provisions related to regulating unsolicited e-mail messages 176
6.4 Commentary on the CAN-SPAM Act 179
6.4.1 Introduction 179
6.4.2 Benefits of the CAN-SPAM Act 179
6.4.3 Criticisms levelled against CAN-SPAM Act 180
6.4.3.1 Pre-emption of state laws 180
6.4.3.2 Regulation, not prohibition 184
6.4.3.3 Limitation of right to claim 185
6.4.3.4 Global nature of spam 187
6.5 Solutions for improvements to the CAN-SPAM Act 188
6.5.1 Technology for enforcement 188
6.5.2 Inclusion of opt-in mechanism 188
6.5.3 A multi-faceted solution 189
6.5.4 International cooperation 190
6.5.4.1 Background 190
6.5.4.2 Memorandum of Understanding between the USA and other countries 190
6.6 Concluding remarks 194
CHAPTER 7 195
A COMPARATIVE STUDY OF ANTI-SPAM LAWS: AUSTRALIA 195
7.1 Introduction 195

7.2 Anti-spam legislation in Australia 195

7.2.1 Background to Australia’s anti-spam legislation 195

7.2.2 Purpose of the Spam Act 196

7.2.3 Anti-spam provisions under the Spam Act of 2003 196

7.2.3.1 Definitions 196

7.2.3.2 Rules for sending electronic mail 198

7.2.3.3 Civil penalties 206

7.2.3.4 Ancillary orders 208

7.2.3.5 Injunctions 209

7.2.3.6 Enforcement of the Spam Act 210

7.2.4 Commentary on the Spam Act 217

7.2.4.1 Background 217

7.2.4.2 Benefits of the Spam Act 217

7.2.4.3 Criticism of the Spam Act 218

7.2.5 Conclusion 220

7.3 Other multi-faceted measures to combat spam 221

7.3.1 Consumer education and awareness 221

7.3.1.1 Recipients 222

7.3.1.2 Businesses 222

7.3.1.3 Public awareness 223

7.3.2 Industry measures 224

7.3.2.1 E-marketing code for spam: A code for ISPs 225

7.3.3 Technological initiatives and solutions 228

7.3.4 International cooperation 229

7.3.4.1 Australia and Korea 230

7.3.4.2 Seoul and Melbourne 231

7.3.4.3 Australia and the Kingdom of Thailand 232

7.3.4.4 Australia, United Kingdom and United States 232

7.3.4.5 Australia and Taipei 233

7.3.4.6 Australia and New Zealand 235

7.4 Conclusion 235

CHAPTER 8 237

A COMPARATIVE STUDY OF ANTI-SPAM LAWS: A SOUTH AFRICAN PERSPECTIVE 237

8.1 Introduction 237

8.2 The ECT Act 25 of 2002 238

8.2.1 Background to the ECT Act 238

8.2.2 The purpose of the ECT Act 239

8.2.3 Consumer protection principles under the ECT Act 239

8.2.4 Data protection principles under the ECT Act 240

8.2.5 Commentary on section 45 of the ECT Act 241

8.2.5.1 Anti-spam provisions under the ECT Act 241

8.2.5.2 Benefits of the anti-spam provisions under the ECT Act 241

8.2.5.3 Criticisms levelled at section 45 of the ECT Act 242

8.2.5.4 Solutions to improve section 45 245

8.2.6 Recent developments that shed light on the spam problem 247

8.2.6.1 Addressing section 45 criticisms through case law 247

8.2.6.2 Self-regulation and the Internet Service Providers' Association (ISPA). 250

8.2.7 Conclusion 252

8.3 Consumer Protection Act 68 of 2008 253

8.3.1 Background to the Consumer Protection Act 253

8.3.2 The purpose of the CPA 254

8.3.3 The consumer's right to privacy 255

8.3.4 Commentary on direct marketing provisions and the right to privacy under CPA 256

8.3.4.1 Definitions 256

8.3.4.2 Direct marketing and the right to privacy 257

8.3.4.3 Opt-out mechanism 258

8.3.4.4 National do-not-call registry 260

8.3.4.5 Enforcement 265

8.3.4.6 Penalties 266

8.3.5 Conclusion 266

8.4 Protection of Personal Information Act 4 of 2013 266

8.4.1 Background to the Protection of Personal Information Act 266

8.4.2 The purpose of the POPI Act 268

8.4.3 Direct marketing and unsolicited communications under the POPI Act 269

8.4.3.1 Section 69: The rights of data subjects regarding direct marketing by means of unsolicited electronic communications, directories and automated decision making……….269

8.4.3.2 Commentary on direct marketing and unsolicited communications under the POPI Act 270

8.4.4 Conclusion 280

8.5 Bills on unsolicited electronic communications 281

8.5.1 ECT Amendment Bill of 2012 281

8.5.1.1 Introduction 281

8.5.1.2 Proposed definition of spam under the Amendment Bill 282

8.5.1.3 Commentary on the anti-spam provisions under the Amendment Bill ... 283

8.5.1.4 Conclusion ... 285

8.5.2 Cybercrimes and Cyber security Bills of 2015 and 2016 ... 285

8.5.2.1 Background ... 285

8.5.2.2 Preamble to the Cybercrimes Bill ... 287

8.5.2.3 Anti-spam-related provisions under the Cybercrimes Bills ... 287

8.5.2.4 Commentary and conclusion ... 294

8.6 Contextualisation of South Africa’s anti-spam and direct-marketing provisions . 296

8.6.1 Introduction ... 296

8.6.2 Overlapping laws ... 296

8.6.2.1 ECT Act and the CPA ... 296

8.6.2.2 ECT Act, CPA and the POPI Act ... 297

8.6.3 Harmonisation of laws ... 297

8.6.3.1 Introduction ... 298

8.6.3.2 Requirements for sending electronic communications ... 298

8.7 Conclusion ... 301

CHAPTER 9 ... 303

RECOMMENDATIONS AND CONCLUSION ... 303

9.1 Summing up the issues ... 303

9.2 A multi-layered approach to combating spam ... 303

9.2.1 Strong legislation ... 304

9.2.1.1 Definition section ... 304

9.2.1.2 Rules for sending electronic communications ... 305

9.2.1.3 Conclusion ... 309

9.2.2 Consumer education and awareness ... 309

9.2.2.1 Background ... 309

9.2.2.2 The role of stakeholders in educating consumers ... 309

9.2.3 Industry initiatives 311

9.2.4 Technological measures 312

9.2.5 International cooperation 312

9.3 Recommendations and conclusion 313

BIBLIOGRAPHY 315

INDEX PAGE 364

CHAPTER 1

BACKGROUND TO THE STUDY

1.1 Introduction

Our era has been variously described in attempts to show how we have evolved from bricks and mortar to technology. Terms including the "information age",[1] "information superhighway";[2] and "global village" have been used to capture the instantaneous ways in which people communicate and transact from remote areas around the world. The Internet,[3] which is able to disseminate information to thousands of recipients in seconds via electronic mail,[4] has also led to an upsurge in electronic commerce.[5] Freed from geographical boundaries, merchants are able to market their goods and services to consumers without limits, while consumers too can access global markets at a click of a

[1] The "information age" is defined as "a period beginning around 1970 and characterised for its nature of publication, consumption and manipulation of information especially by computers and computer networks". The Free Dictionary 'Information age' http://www.thefreedictionary.com/information+age (date of use: 7 September 2015).

[2] "Information superhighway" refers to "the global information and communication network that includes the Internet and other networks and switching systems such as telephone networks, cable television networks, and satellite communications networks". It is also described as "the Internet bulletin board services, online services, and any other services that enable people to obtain information from telecommunications networks". Margolis *Computer & Internet Dictionary* 273; and Free Dictionary 'Information superhighway' http://www.thefreedictionary.com/information+superhighway (date of use: 7 September 2015).

[3] The "Internet" is a "global network connecting millions of computers. It is also defined as a cooperative message-forwarding system linking computer networks all over the world. Users of the Internet can exchange electronic mail, participate in electronic discussion forums (newsgroups), send files from any computer to the other via file transfer protocol (FTP), retrieve information via Gopher or Hypertext transfer protocol (HTTP), and even use each other's computer directly via Telnet". See Downing, Covington & Covington *Dictionary* 243; also Margolis *Computer & Internet Dictionary* 283; and Oxford *Dictionary of Computer Science* 279.

[4] "Electronic mail", or otherwise referred to in its short form as "e-mail", is "the transmission of messages over communications networks" (Margolis *Computer & Internet Dictionary* 190); or "messages sent between computer systems, the computer systems being used to hold and transport messages" (Oxford *Dictionary of Computer Science* 184). The terms electronic mail, e-mail, and e-mail messages are used interchangeably save where specific anti-spam legislation assigns a different meaning to them.

[5] "Electronic commerce" or "e-commerce" is defined broadly as "the use of electronic networks to exchange information, products, services and payments for commercial and communication purposes between individuals (consumers) and businesses, between businesses themselves, between individuals themselves, within governments, or between the public and government, and between business and government". Department of Communications (Republic of South Africa) *Green Paper on Electronic Commerce: Making it your own business* (2000) 9.

mouse, 24/7, 365 days a year enabling them to transact and communicate freely and in a relaxed environment. However, the Internet has also made it possible for dubious characters and unsavoury activities to thrive, thereby exposing consumers to a variety of dangers. Among these dangers are deceptive practices used by marketers, which include the dissemination of unsolicited electronic communications and also access to consumers' private information, for use in marketing their goods and services. This has, in turn, made it difficult for consumers to safeguard their private information while transacting or communicating online.

The practice of sending unsolicited electronic communications – otherwise known as spamming – has been termed the "scourge of the 21st century".[6] Spamming takes place when marketers or senders of spam ("spammers") bombard consumers with products or services without the consent of those consumers. Because the spam e-mails are unannounced, uninvited, and from different sources, spamming has been said to compromise the convenience of e-mail.[7]

Statistics reveal that spam was a problem in South Africa as far back as 2003 when 74 per cent of South African consumers stated that they were unsettled by unsolicited advertising.[8] Of the marketing community polled in that year, "72 per cent indicated that they found spam more problematic than viruses and hacking threats".[9] In 2004, a further

[6] Cerf V ISOC Chairman (acknowledged as the father of the Internet), as quoted in Everett-Church R 'Why spam is a problem' http://www.isoc.org/oti/articles/0599/everett.html (date of use: 7 September 2015).

[7] Rao JM & Reiley D 'The Economics of spam' 1-25 http://www.davidreiley.com/papers/SpamEconomics.pdf (date of use: 7 September 2015).

[8] Tin Can Communications 'Unsolicited advertising material bothers 74% of South African consumers' http://www.bizcommunity.com/Article.aspx?c=19&1=196&ai=1877 (date of use: 7 September 2015). In this survey the following concerns were outlined "77% of respondents said companies send too much unsolicited advertising; 57% said they are not happy to receive information from companies with which business has not been done before; 62% said they do not bother to receive telephone calls selling products or services; 65% said many companies call consumers at their homes to sell them products and services".

[9] Systems Publishers 'South African spam summit announced' http://www.bizcommunity.com/Article.aspx?c=16&1=196&ai=2347 (date of use: 7 September 2015). The Spam Summit revealed that spam had caused South African businesses between R7 and R13 billion per annum in terms of lost productivity; also Burger & Rensleigh (2007) 9/3 *South African Journal of Information Management* http://www.sajim.co.za/default.asp?to=peer1vol9nr3 (date of use: 7 September 2015).

report revealed that a growing number of South African companies were using e-mail as an important component of their online marketing strategies, and that between 45 and 60 per cent of all e-mail messages sent were spam e-mails.[10] In 2007 spam had risen to 95 per cent of online communications.[11] By 2012 the e-mail spam percentage in South Africa revealed that "one in every 436,6 e-mails was considered malicious and carried a virus;[12] and that 1 in every 1,48 e-mail was considered spam".[13] This made up 67,8 per cent of all South African e-mail traffic during July of 2012.[14] In 2014 it was reported that spam accounted for 80 per cent of global e-mail traffic.[15]

The question, then, is if spam accounts for the amount of traffic noted above, how do spammers or marketers obtain consumers' e-mail addresses which enable them to solicit consumer support for their products and services? This, they do in various ways, notably by profiling consumers when they browse the web. Spammers also use dictionary attacks to extract e-mail addresses from web sites and also harvest such. Once the spammer has such lists, he or she can send spam e-mails to an undisclosed number of recipients, and (in most cases) remain undetected by using third parties' domain names or false headers when sending those e-mails.[16] The inability of consumers to locate spammers also creates problems which impact on a variety of

[10] Idea Engineer 'Ask before you send marketing e-mail' http://www.biz-community.com/Article.aspx?c=16&1=196&ai=2969 (date of use: 7 September 2015).

[11] Mann J 'Spam is 95% e-mail traffic says Barracuda' http://www.techspot.com/news/28226-spam-is-95-of -e-mail-traffic-says-barracuda.html (date of use: 7 September 2015).

[12] Proome J 'SA e-mail spam percentage revealed' http://mybraodband.co.za/news/security/58901-sa-e-mail-spam-percentage-revealed.html (date of use: 7 September 2015).

[13] Ibid.

[14] Ibid.

[15] ITU 'ITU and Internet Society collaborate to combat spam' http://www.itu.int/net/pressoffice/press_releases/2014.aspx#.VIvi-E1DGpo (date of use: 7 September 2015); also Spamhaus 'The world's worst spammers' http://www.spamhause.org/statistics/spammers (date of use: 7 September 2015). According to Spamhaus the spammers list is based on the following: "the view that spammers or spam gangs cause the highest threat; are the least repentant; are most persistent; and cause the most damage on the Internet currently"; and AVTest 'Spam' https://www.av-test.org/en/statistics/spam for the origins of spam per country (date of use: 7 September 2015).

[16] In January 2014 when the new generic top level domain (gTLD) program for the registration of new generic top-level domains was launched, it was noted that spammers were quick to utilise domain names for the distribution of largescale advertising spam (see Shcherbakova T, Vergelis M & Demidova N 'Spam and phishing in the first quarter of 2015' https://securelist.com/analysis/quarterly-spam-reports/69932/spam-and-phishing-in-the-first-quarter-of-2015 (date of use: 7 September 2015).

stakeholders, including: Internet service providers (ISPs); businesses; and consumers themselves. For consumers, these problems include the inconvenience of having to wade through spam e-mails before reading their legitimate mail, and the need to pay elevated subscription fees to accommodate the increased storage capacity required for those unwanted e-mails.[17] The ISPs, on the other hand, can incur revenue loss and loss of business opportunities, as well as damage to computer equipment where bandwidth is insufficient to handle the congestion created by spam.[18] Other costs include the installation of filtering software,[19] or any other software that can assist in limiting spam.[20]

While these initiatives have proven effective in dealing with some of the problems caused by spam, they have been unable entirely to eliminate this scourge. In fact, the technical measures have merely revealed loopholes on which spammers have been quick to capitalise. In an effort to combat spam, international organisations such as the International Telecommunications Union and the Organisation for Economic Cooperation and Development have from the early 2000s to the present day, made valuable contributions in this regard.[21]

Regional communities, with specific focus on the African region: the African Union (AU), and its regional economic communities (RECs) such as the Common Market for Eastern and Southern Africa (COMESA), and Southern African Development Community (SADC) have added their voice to the discussions by drafting Model Laws and Conventions and finding ways in which to work towards harmonising their existing laws aimed at combating spam.

While the international arena was conducting its research into the issue, some countries had anti-spam laws in place, and/or anti-spam provisions in existing legislation. Although the first specific anti-spam legislation was adopted in 1997, this was a “state”

[17] Schryen *Anti-spam Measures* 22-8 for a discussion on the economic loss caused by spam.

[18] Ibid.

[19] Technical measures to eliminating spam will be covered in Chapter 3.

[20] These problems will be discussed at length in Chapter 3.

[21] Commonly abbreviated and hereafter cited as the ITU and the OECD respectively.

initiative within the United States of America (USA) and did not apply nationally.[22] Anti-spam laws at national level started taking shape in the 2000s.[23] Japan led the way, quickly followed by the USA, Australia, and other players.[24] South Africa is among those countries that had provisions regulating spam in the early 2000s.

1.2 Scope and purpose of this study

1.2.1 Title

The title of this thesis is: "THE REGULATION OF UNSOLICITED ELECTRONIC COMMUNICATIONS (SPAM) IN SOUTH AFRICA: A COMPARATIVE STUDY".

1.2.2 Study objectives

The aim of this thesis is to analyse whether the legal mechanisms established to protect consumers from the receipt of unsolicited electronic communications in South Africa are adequate. The feasibility of harmonising the current anti-spam provisions to provide better protection for consumers will be considered. Further, an assessment of whether the introduction of requirements for the dissemination of unsolicited electronic communications into existing legislation is feasible.

1.2.3 Research question

[22] The anti-spam legislation in the USA both at state and federal level is discussed in Chapter 6 below.

[23] See, in particular, Lynch K 'Timeline of spam related terms and concepts' http://keithlynch.net/spamline.html (date of use: 5 November 2015). There are currently over sixty countries which regulate spam by legislation in their respective jurisdictions. This regulation is done through fully-fledged legislation or alternative legislation (pre-existing legislation). Spamlaws 'How to stop scams and fraud' http://www.spamlaws.com (date of use: 7 September 2015); also Schryen *Anti-spam measures* 17.

[24] See Law on Regulation of Transmission of Specified Electronic Mail Act passed April 2002, amended in 2005 and 2008 http://www.mofo.com/resources/publications/2008/07/japanese-new-anti_spam.law (date of use: 7 September 2015). Canada has recently passed its anti-spam law namely: Canada Anti-Spam Legislation (CASL) of 2014 (see Canadian Radio-television and Telecommunications Commission 'Canada's Anti-spam Legislation' http://crtc.gc.ca/eng/internet/anti.htm (date of use: 7 September 2015). This thesis will however, focus on the USA and Australia which will be discussed in detail below.

The question is asked whether the current overlapping and minimalist anti-spam and direct marketing provisions protect consumers adequately. Likewise, will the introduction of restrictive legislation adequately protect online consumers from receiving spam? Finally, the question as to whether a multi-faceted approach in combating spam with the introduction of a Model Law would be a suitable starting point in aligning with international best practices to combat the act of spamming is addressed.

1.2.4 Hypothesis

This thesis works on the assumption that spam is harmful and should be curbed. It is also accepted that the current, inadequate consumer protection measures can be improved. All measures adopted need to reflect a multi-faceted approach to curbing spam which will include all affected stakeholders in an effort to realise a holistic approach. This approach will start with an anti-spam law setting out basic requirements that can sufficiently protect consumers from receiving unsolicited electronic communications. And as spam is a global problem, South Africa needs to look at the option of entering into mutual agreements with other countries and organisations in order to combat spam at a global level.

1.2.5 Rationale of the thesis

The study is undertaken, in the main, by means of a literature review reflecting an analysis of the various legal instruments regulating the issue of spam such as: consumer protection laws; credit laws; data protection laws; cybersecurity and cyber-crimes legislation, in particular. This is undertaken to establish whether those laws can be harmonised in order to regulate spam. Given the comparative nature of the study, domestic, international, and foreign materials are used. In addition, both hard and soft law instruments will be consulted.

1.2.6 Parameters

It should be noted at the onset that the term spam has been variously described – for example, as unsolicited bulk communications; unsolicited bulk commercial e-mail; unsolicited commercial communications; unsolicited commercial electronic mail; unsolicited electronic communications; and unsolicited electronic communications. Focus will be on spam as generally described in anti-spam laws. The above terms will also be used interchangeably throughout the thesis.

As spam is a multi-faceted problem affecting different stakeholders, it follows that focus will be on specific issues to keep the thesis manageable. Focus will solely be on consumers as recipients of spam from either spammers or businesses engaging in direct marketing practices. The terms consumers; individuals; recipients; and end users will be used interchangeably throughout the thesis. Focus will also be on ISPs and their role in protecting consumers from receiving spam.

The above will be followed by a discussion on the international and regional arenas to establish the initiatives so far taken to combat spam. While there are a number of international organisations dealing with this issue globally, the ITU and the OECD's contribution is the main focus of this study. That will be followed by regional initiatives and the contribution made by the AU, COMESA, and SADC.

A comparative study is also undertaken to establish how the jurisdiction below have been regulating spam. The comparative analysis will therefore be limited to three jurisdictions, namely the USA, Australia, and South Africa. The comparative study will focus on the differences and similarities in the chosen legal systems. It will analyse the content of the rules in each of the selected jurisdiction, and the manner in which they address the issue of spam.[25] The similarities and differences will then be used to draw lessons for South Africa which follows a minimalistic approach with regards to spam.

Spam overlaps with a number of constitutional provisions such as the right to conduct business freely (which relates mainly to markerters and or spammers). However, the

[25] See generally Kothari *Research Methodology: Methods and techniques* 1 ff.

constitutional provision on the right to privacy which is also given effect to by the Protection of Personal Information Act of 2013 will be examined in this thesis. Of equal importance is the consumers' fundamental right to privacy under the Consumer Protection Act of 2008.

Finally, while traditionally spam has been sent via newspapers (junk mail), printed catalogues, et cetera, the evolving modes of communication such as e-mail; mobile phones, are now perpetuating the scourge. This study focuses, in the main, on spam distributed via e-mail including e-mails accessed by phones. Reference is made to mobile spam, only when necessary.

1.3 Synopsis: Chapter trajectory

Chapter one, this introductory chapter, establishes the scope and purpose of the study.

In **Chapter two,** focus will be on a discussion of direct marketing and the development of spam in the context of the Internet. The concept of direct marketing will be outlined and a comparison of traditional marketing and online marketing will be made; the development of spam via electronic communications with special focus on commercial and non-commercial spam; and lastly, the benefits spamming holds for spammers.

Chapter three focuses on the effect of spam on e-mail messages under the headings: the methods used to extract e-mail addresses in order to send spam; problems resulting from spam; technical measures used to combat spam; and spam fighters.

In **Chapter four** an evaluation of international initiatives to combat spam through an examination of international guidelines and model laws adopted by the international community will be outlined. The chapter focuses on initiatives of the ITU and the OECD aimed at the regulation of spam, and the background history of each organisation; initiatives taken to combat spam; and the documents, surveys, guidelines, and toolkits of those respective organisations are reviewed.

Regional initiatives are addressed in **Chapter five** with emphasis falling on African initiatives, most notably those of the AU as an organisation, and its regional communities (RECs). Because South Africa is located within this region, the SADC and COMESA as the RECs will be at the centre of this discussion.

A study of this nature calls for a comparative element if issues are to be viewed in perspective. The trends in selected jurisdictions are discussed to establish how they have been combating spam. An essential part of this study involves an evaluation of the potential efficacy of the opt-out mechanism in contrast to opt-in mechanism for combating spam. Focus falls mainly on how these two mechanisms compare, and whether one is more effective than the other. As noted above the following anti-spam laws will be considered: the USA; Australia; and anti-spam provisions in South Africa will be considered which apply the above mechanisms respectively. All three jurisdictions have outlined basic requirements for sending unsolicited electronic communications in their legislation or anti-spam provisions. These include definition(s) describing what constitutes spam. These jurisdictions also enforce the provisions differently. Spam is not only legislated at a national level, but the jurisdictions have also entered into mutual agreements with other countries and organisations in an effort to combat spam at a global level, with the exception of South Africa.

Chapter six opens the comparative study with an analysis of the USA's anti-spam laws. The discussion of spam in the USA starts with the regulation of spam at state level. The requirements adopted on how to send electronic communications are addressed as outlined in state laws. How states define spam is highlighted and the mechanisms each state employ in regulating spam will be considered. A discussion on the prohibitions in those anti-spam laws will be highlighted. Case law is used to illustrate how state anti-spam laws have been interpreted by the courts.

The USA enacted its national anti-spam law namely: The Controlling the Assault of non-solicited Pornography and Marketing Act (CAN-SPAM Act) in 2003. This law has a pre-emptive clause on most state laws, some of which were considered to be very restrictive in combating spam. In addressing the Federal law the following is considered: the background to the Act and its purpose; an outline of and commentary on the Act which includes the benefits of the Act; some criticisms levelled against the Act by commentators; and suggestions for improvement. Consideration is also made of the mutual agreements between the USA and other countries and/or organisations aimed at combating spam at a global level. This is done taking case law into consideration. It must be noted that the CAN-SPAM Act utilises the opt-out mechanism.

The comparative study continues in **Chapter seven** which focuses on Australia's anti-spam law. The Australian Spam Act was passed into law in 2003. Australia follows a five point approach to spam. The discussion will therefore focus on the following: the provisions of the Spam Act; a commentary on the Act covering the benefits of the Act, criticism of the Act by commentators, and suggestions for improvement. Other approaches are also addressed including: consumer education; technical measures; industry body; and mutual agreements. It should be noted that Australia follows a restrictive approach in dealing with spam – for example, an opt-in mechanism.

In **Chapter eight** focus will be on anti-spam initiatives in South Africa. South Africa does not have a specific anti-spam law, but anti-spam provisions scattered thoughout a number of legislations. In the main, these provisions overlap, leave gaps, and offer consumers only meagre protection. The first anti-spam provisions in South Africa was adopted in the Electronic Transactions and Communications Act.[26] This was followed by other provisions relating to consumer credit;[27] consumer protection;[28] and most recently, legislation on the protection of personal information.[29] In 2012, 2015 and 2016 respectively, a number of Bills were published: one proposing amendments to, inter alia, the anti-spam provisions in the ECT Act of 2002;[30] and the other two Bills are on

[26] Electronic Communications and Transactions Act 25 of 2002.

[27] National Credit Act 34 of 2005.

[28] Consumer Protection Act 68 of 2008.

[29] Protection of Personal Information Act 4 of 2013.

[30] See Electronic Communications and Transactions Amendment Bill (*GG* No. 888 of 2012).

Cybercrimes and Cyber security.[31] In addition to the above an industry body regulating ISPs was established in 2006 to deal with matters affecting ISPs.[32] The regulation of spam falls within its mandate. In this chapter the South African legislation which includes the above anti-spam provisions will be discussed. A background study on each piece of legislation; the purpose of that particular legislation; and other provisions relating to the study are highlighted. This is followed by an outline of the anti-spam and direct marketing provisions in those laws; commentary on that particular provision; criticism levelled against the provision (if any); and solutions to those criticisms (if any) are also highlighted. Case law is called into service to show how some provision(s) have been interpreted by our courts of law.

This discussion includes published Bills which contain spam related provisions. The issue of industry regulation is also highlighted in this chapter. The chapter concludes with a commentary on the contextualisation of these laws to compare and contrast them, and to see whether a harmonisation of these laws can offer a point of departure for the regulation of the issue of spam in South Africa.

In **Chapter nine** the discussions above will be drawn together and recommendations will be offered as to the most feasible and effective approaches to the regulation of spam in South Africa. It is hoped that through this study South Africa will be able to work towards a multi-faceted approach to combating spam which will start with the harmonisation of its fragmented system. Most importantly an introduction of a proposed Model Law aimed at regulating spam within borders and also offers solutions at a global level will be outlined.

[31] See Cybercrimes and Cyber security Bill: Draft for public comment (*GG* of 2015); and Cybercrimes and Cybersecurity Bill (*GG* No. 40487 of December 2016).

[32] Guidelines for Recognition of Industry Representative Bodies of Information System Providers' "(IRB Code)" GN 1283 *GG* 29474 of 14 December 2006).

CHAPTER 2

DIRECT MARKETING AND THE DEVELOPMENT OF SPAM VIA ELECTRONIC COMMUNICATIONS

2.1 Introduction

Consumers are vital to the success of any economy. In an effort to understand consumers, businesses have resorted to studying them and, most importantly, to manipulat their behaviour.[1] Marketing companies also use spam e-mails offering various options to persuade consumers to engage with them. These options include the sale of goods, services, dissemination of information, and ideas, et cetera.[2]

Because of South Africa's history, the majority of consumers are largely uneducated as regards their rights. Hence recent laws are aimed at remedying those shortcomings.[3] However, the age of technology plays its own part in perpertuating, indeed exacerbating, an unequal society in which the marketer is the "guru" and the consumer the "apprentice", forever learning but always lacking sufficient wisdom and foresight. The new mediums are used to manipulate consumers and to influence them to act emotionally rather than rationally when faced with the advances in marketing.[4]

In this chapter direct marketing as a concept and a comparison between traditional marketing and online marketing is addressed. This is followed by an analysis of the development of spam in an online environment with special focus on the different types

[1] Cant & Van Heerden *Marketing Management* 12-13.

[2] Id 1-29.

[3] See, in particular, the following: section 3 (a) of the National Credit Act, 2007 which provides as its purpose: "to promote and advance the social and economic welfare of South Africans by promoting a fair, transparent, competitive, sustainable, responsible, efficient, effective and accessible credit market and industry. This is achieved by promoting the development of a credit market that is accessible to all South Africans, and in particular to those who have historically been unable to access credit under sustainable market conditions." The preamble to the Consumer Protection Act 68 of 2008 on the other hand notes: "that apartheid and discriminatory laws of the past have burdened the nation with unacceptably high levels of poverty, illiteracy, and other manifestations of social and economic inequality; and also it is necessary to develop and use innovative means to promote, among others: the interests of all consumers; to ensure accessible, transparent, and efficient redress for consumers who are subjected to abuse or exploitation in the marketplace".

[4] Cant & Van Heerden supra n 1 411-13 on cyber marketing.

of spam e-mails disseminated in that environment. The chapter concludes by outlining the benefits that spammers derive from such practices.

2.2 Direct marketing

Marketing in general is a broad concept with different meanings for different people. It can, however, be defined as "a process where an organisation in its drive to meet its goals, focuses on meeting consumer needs and wants by offering the right product at the right price, at the right place, and through the right marketing communication channels".[5] In that process marketers strive to establish relationships with consumers and to develop and grow these relationships with relevant stakeholders in an ever-changing environment.[6] Ultimately, the aim of marketing is to know and understand the customer so well that the product and service offered fits that individual and sells itself.[7] Ideally this results in a customer who is ready to engage with those marketing tactics because all that a marketer is looking for is to have the product or services available for that consumer and to make a profit.[8]

Direct marketing, on the other hand, is a management concept – a multi-level communication and distribution tool.[9] It involves a variety of activities including: direct mail and direct response advertisements through that mail;[10] telemarketing;[11] database

[5] Id 19.

[6] Id 2-3 and 19.

[7] Id 19-20

[8] Ibid.

[9] "Direct marketing" is also defined as "a form of advertising in which physical marketing materials are provided to consumers in order to communicate information about a product or service. Direct marketing removes the 'middle man' from the promotion process, as a company's message is provided directly to potential consumers". Investopedia 'Definition of direct marketing' http://www.investopedia.com/terms/d/direct-marketing.asp (date of use: 5 November 2015).

[10] "Direct mail" is a "process of sending out sales letters or other materials through the mail to potential consumers or clients. Direct mail campaigns may be directed to either consumers or the business market". Duermyer R 'Direct mail defined' http://homebusiness.about.com/od/homebusinessglossar1/g/direct_mail_def.htm (date of use: 5 November 2015); and Hamman & Papadopoulos (2014) 47/1 *De Jure* 44-5 for examples of direct marketing.

[11] "Telemarketing" or "telesales" is "an act of marketing goods and services to potential consumers over the telephone, by either telemarketers or by automated telephone calls or "robocalls". Telemarketing can be intrusive and also perpetrates scams and fraud". Investopedia 'Definition of telemarketing' http://www.investopedia.com/terms/t/telemarketing.asp (date of use: 5 November 2015); and Bizcommunity 'Telemarketing rings true in South Africa'

management;[12] the Internet;[13] information, communication and technology;[14] and mobile commerce.[15] All these activities aim to stimulate the target audience to take immediate action and to create an individualised customer relationship.[16] Although this definition is broad and encompasses a number of categories, focus is limited to Internet marketing as it relates to spam. The definition also covers both traditional and electronic marketing which is discussed below.

2.2.1 Traditional marketing versus electronic marketing

2.2.1.1 Background

The direct marketing activities above outlines the traditional way of doing business (bricks and mortar) and that of an online environment. In a traditional market the consumer could feel, touch and examine the goods he or she intended to purchase before buying those products. This has changed in that while consumers in an online

http://www.bizcommunity.com/Article/196/14/118519.html (date of use: 5 November 2015), on the rising success of telemarketing.

[12] "Data management" is defined as "a computer program that catalogues, indexes, locates, retrieves, and stores data, maintains its integrity, and outputs it in the form desired by a user". A "data management system (DBMS)" sometimes called "data manager", is a program that "lets one or more computer user create and access data in a database. The DBMS manages user requests (even requests from other programs) so that users and other programs know where the data is physically located on storage media and in multi-user system. In handling user requests, the DBMS ensures the integrity of the data (making sure it continues to be accessible and is consistently organised as intended) and security (making sure that only those with access privileges can access the data)". BusinessDictionary.com 'Database management system (DBMS)' http://www.businessdictionary.com/definition/database-management-system-DBMS.html (date of use: 5 November 2015).

[13] "Internet marketing" refers to "the application of marketing principles and techniques via electronic media and more specifically the Internet". Quirk 'What is eMarketing and how is it better than traditional marketing?" https://www.quirk.biz/resources/88/What-is-eMarketing-and-how-is-it-better-than-tradional-marketing (date of use: 5 November 2015); Cant & van Heerden supra n 1 411-14 and 425-6; and Sterne & Priore *Email Marketing* 1 ff.

[14] Hereafter referred to as "ICT". See Kokt & Koelane (2013) 7/3 *African Journal of Business Management* 3098-9.

[15] "Mobile commerce", or "m-commerce" is "the use of wireless handheld devices such as cellular phones and laptops to conduct commercial transactions online". Investopedia 'Mobile commerce' http://www.investopedia.com/terms/m/mobile-commerce.asp (date of use: 5 November 2015). For a discussion on mobile commerce see: Papadopoulos 'Online Consumer Protection' 63-4 on the rise of m-commerce; also Jobodwana (2009) 4/4 *Journal of International Commercial Law and Technology* 287 ff; and the following on mobile marketing: Rowles *Mobile Marketing* 9 ff; Petzer (2011) 8 *Journal of Contemporary Management* 384 ff; Krum *Mobile Marketing* 1 ff; Jansen van Ryssen (2004) 4 *Acta Commercii* 48 ff.

[16] Id Krum 5-12; and Rowles 24.

environment can still see the product they are interested in, they can no longer feel, and touch such a product. In the discussion below the comparison between traditional and electronic marketing is highlighted.

2.2.1.2 Comparison between traditional marketing and electronic marketing

The differences cover aspects such as modes of delivery, tools used to market products or services, and costs accompanying such marketing strategies. The terms "online marketing", "Internet marketing", and "electronic marketing" are used interchangeably in this section. In comparing traditional and electronic marketing the following important aspects emerge:[17]

(a) *Relationship*. Traditionally a relationship was established once the consumer(s) had made contact or had responded to an offer of goods and or services from a particular merchant. In an online environment contact can be made without the establishment of a relationship.

(b) *Costs.* In traditional marketing the high costs of advertising are incurred by the marketing companies who distribute the advertisements. These costs include: postage for "snail mail"; the cost of broadcasting time when TV adverts are involved; newspaper space for advertisements; or phone calls (in the case of telemarketing). Online marketing costs have shifted to the recipients and ISPs.[18]

(c) *Traceability*. In traditional marketing the company includes a return address in its correspondence with the recipient in case that recipient would like to opt-out of receiving further mail from that particular business. In online marketing, the

[17] See the following for a general comparison of traditional and electronic marketing: Li (2006) 3/1 *Webology* 1-13 http://webology.ir/2006/v3n1/a23.html (date of use: 5 November 2015); and Quirk 'What is eMarketing and how is it better than traditional marketing?' https://www.quirk.biz/resources/88/What-is-eMarketing-and-how-is-it-better-than-traditional-marketing (date of use: 5 November 2015).

[18] The issue of costs is discussed in Chapter 3 below.

unsolicited mail, in most cases, provides no return address which would allow the recipient to opt-out of receiving further unwanted mail.

(d) *Deterrence.* In traditional marketing deterrence or punishment is an important cosideration as the sender is easily traceable. In online marketing deterrence is weak in that punishment depends on detecting the person responsible for sending the unsolicited mail. Prosecuting spammers is difficult as they often use third-party domains to send spam e-mails thus making it hard to trace.

(e) *Information*. Traditionally, consumers provided personal information voluntarily as they wished to establish contact with a particular merchant. In an online environment, by contrast, when consumers browse the Internet their personal information is often captured without their knowledge – for example, through cookies in a web site.[19] Once that personal information has been gathered it can either be sold to third parties dealing in such information, or the consumer can end up receiving even more spam.[20]

(f) *Reliability*. In traditional marketing the snail mail might sometimes go missing or simply not be delivered. The consumer might even decide to discard the mail as it is clear from the mail itself who it is from. In online marketing the consumer might not be able to determine the origin of the e-mails in that spammers or marketers frequently disguise their headers.

(g) *Boundaries*. Traditional marketing is sometimes territorial in nature – ie, it is limited by boundaries. Online marketing, on the other hand, is borderless and consumers are not only available 24/7, but are also accessible via the Internet from all over the world.

(h) *Delivery mode*. Traditionally marketing information would be communicated to consumers either by snail mail, telephone, newspapers, TV, radio, catalogues,

[19] This is discussed in Chapter 3 below.

[20] The issue of profiling is dealt with in Chapter 3.

et cetera. Marketing was limited as businesses could not reach each and every individual. In an online environment the middleman has been eliminated guaranteeing targeted and personalised delivery from the marketer to the consumer.[21]

(i) *Accessibility*. Traditional marketing is not always accessible as there might be barriers. On the other hand, online marketing is accessible almost instantaneously.

(j) *Mediums of communication*. With traditional marketing communication is mainly via post, TV, newspapers, catalogues, and telephone. Online marketing takes place mainly on the Internet using e-mail, and, also short messaging system. [22]

The above differences reveal how marketing has evolved by eliminating barriers such as, location and time. This environment allows the marketer to be in close contact with and monitors the consumer around the clock. This has, in turn, exposed the consumer to dangers that were not there before, for example, receiving unsolicited communication, or spam. Hereafter follows a discussion on how spam developed in the electronic environment.

2.3 Development of spam via electronic communications

2.3.1 Background

The Internet has indeed changed the way in which business is being conducted online. This has not only introduced new mediums of communications for ease of communicating but it has also brought about new challenges. The term "electronic communication" refers to the transfer of writing, signals, data, sounds, images

[21] Krum supra n 15 6-7.

[22] "Short messaging system" or "SMS" is used to send text messages to mobile phones. The messages can be up to 160 characters in length. TechTerms 'SMS' https://techterms.com/definitions/sms (date of use: 10 November 2015).

conducted via an electronic device.[23] The use of e-communications allows people to interact in different ways via mediums such as e-mails and SMSs et cetera.[24] These mediums have been utilised by spammers and marketers alike to send unsolicited mail to unsuspecting recipients.

Although the phenomenon of sending unsolicited e-mail has been around for some time, it is still unclear when spam became the nuisance it is today. Some are, of the opinion that electronic junk mail became known as spam because of the Monty Python skit on spam in the 1970s.[25] In this skit a group of Vikings sang a chorus of “SPAM, SPAM, SPAM” at increasing volumes in an attempt to drown out other conversation.[26] This is today evident in mailboxes as spam drowns out legitimate e-mails. By the 1990s, concepts such as: “unsolicited commercial e-mail” (UCE), “mass dissemination of Netnews” and “unsolicited bulk mail” (UBE) were used to describe spam within an electronic environment.[27] Later in the 2000s some of these concepts formed part of the definitions of spam in most anti-spam legislation. In the discussion below focus will be on the evolution of spam via electronic communication.

2.3.2 The evolution of spam via electronic communication

2.3.2.1 ARPAnet and the first signs of junk mail (spam)

Before junk mail was referred to as spam, Jon Postel[28] observed the following in a report on the problem of junk mail:[29]

[23] Hereafter referred to ‘e-communications’. See Reference ‘What is e-communication?’ https://www.reference.com/technology/e-communication-9e8fce72a6a417a3# (date of use: 21 March 2017).

[24] Ibid.

[25] Glasner J ‘A brief history of spam and spam’ http://www.wired.com/2001/05/a-brief-history-of-spam-and-spam (date of use: 5 November 2015); also Fletcher D Time ‘A brief history of spam’ https://content.time.com/time/business/article/0,8599,1933796,00.html (date of use: 10 November 2015); Tladi (2008) 125/1 *SALJ* 179; and Geissler *Bulk Unsolicited Electronic Messages* 16.

[26] Ibid.

[27] Lynch K ‘Timeline of spam related terms and concepts’ http://keithlynch.net/spamline.html (date of use: 5 November 2015).

[28] John Postel was an American computer scientist who helped launch ARPAnet in the 1960s. He is regarded as one of the Internet pioneers. Internet Society ‘A ten year tribute to Jon Postel’ http://www.isoc.org/awards/postel/memory.shtml (date of use: 5 November 2015).

> The ARPA Network[30] Host/IMP[31] interface protocol there is no mechanism for the “Host” to selectively refuse messages. This means that the Host which desires to receive some particular message must read all messages addressed to it. Such Host could sent many messages by a malfunctioning Host. This would constitute a denial of service to the normal users of this Host. Both the local users and the network communication could suffer. The services denied are the processor time consumed in examining the undesired messages and rejecting them and the loss of network thruput (throughput) or increased delay due to the unnecessary busyness of the network. It would be useful for a Host to be able to decline messages from sources it believes are misbehaving or are simply annoying. If the Host/IMP interface protocol allowed the Host to say to the IMP “refuse messages from Host X”, the IMPs could discard the unwanted messages at their earliest opportunity returning a ‘refused’ notice to the offending Host.

This is a blueprint of the modern day spam, outlining the problems caused by spam such as burdening infrastructure and also denying service to normal users (recipients) of the host. The terms “host” and “malfunctioning host” is the modern day recipients of spam and those that send spam emails can either be spammers or marketers themselves who partake in spamming activities.

Mention was, however, made of how a host could discard unwanted messages, and two possibilities were identified:[32]

> The destination IMP would keep a list (per local Host) of sources to refuse (this has the disadvantage of keeping the network busy). The destination IMP on receiving the “refuse messages from the Host X” message forwards the message to the source IMP (the IMP local to Host X). That IMP keeps a list (per local Host) of destinations that are refusing messages from this source Host. This restriction on messages might be removed by a destruction Host either by sending a “accept messages from Host X” message to the IMP, or by resetting its Host/IMP interface. A Host might make use of such facility by measuring per source the number of undesired messages per unit time if this measure exceeds a threshold then the Host could issue the ‘refuse messages from Host X’ message to the IMP.

[29] Postel J ‘On the junk mail problem’ Network Working Group (SRI-ARC) Request for Comment 706 (Nov 1975) NIC #33861 http://www.rfc-archive.org/getrfc.php?rfc=706 (date of use: 5 November 2015).

[30] ARPAnet or ARPA Network which stands for Advanced Research Projects Agency Networks was a precursor to the Internet. It was a large wide-area network created by the United States Defense Advanced Research Project Agency (ARPA). ARPAnet was established in 1969 and served as a testbed for networking technologies, linking many universities and research centers. Webopedia ‘Arpanet’ http://webopedia.com/TERM/A/ARPANET.html; and Internet Society ‘Brief history of the Internet’ http://www.internetsociety.org/internet/what-internet/history-internet/ brief-history-internet (date of use: 5 November 2015).

[31] An IMP stands for “interface message processor” and it is noted as “having been the first packet router. It was part of the ARPAnet and is a precursor to the Internet”. Technopedia ‘Interface Message Processor (IMP) https://www.technopedia.com/definition/7692/interface-message-processor-imp (date of use: 18 March 2017).

[32] Postel ‘On the junk mail problem’ supra n 29.

The above are the modern-day technical measures that have been put in place to combat spam, which include the use of filters. It is clear that before spam became the scourge it is today, it was viewed as a potential problem, and that while the concern was about a host malfunctioning, today this might easily refer to spammers or marketers sending unwanted e-mail.

2.3.2.2 Types of spam messages in an electronic environment

Spam comes in different forms, in the main masquerading as legitimate e-mail, enticing consumers to view something that might interest them. There are two broad types of spam e-mail: commercial and non-commercial.

(a) Non-commercial spam

Non-commercial spam, unlike its commercial counterpart, is characterised as a "nuisance" or "annoyance". Although non-commecial spam does not attempt to sell anything, it does in most cases "prompt the receiver to do something about the e-mail – it elicites an emotional response from the recipient".[33] Non-commercial spam includes, but is not limited to: chain letters (urban legends, hoaxes and viruses),[34] and petitions, each of which is discussed separately.

Chain letters

A chain letter is "a written text which advocates its reproduction by requiring the recipient to forward the e-mail to multiple recipients,[35] usually with the promise of good luck".[36] Chain letters have been in existence for centuries, first as snail mail, then as

[33] See Snopes.com 'Chain linked' http://www.snopes.com/luck/chain.asp (date of use: 5 November 2015).

[34] Ibid.

[35] Emery D 'What is a chain letter?' http://urbanlegends.about.com/od/internet/f/chain_letter.htm (date of use: 5 November 2015).

[36] The promise of good luck depends on what the recipient is asked to do. There are different consequences for each request, some good some bad. Rutgers 'Chain letters' http://www.cs.rutgers.edu/~watrous/chain-letters.html (date of use: 5 November 2015).

faxes, and currently in the form of e-mail.[37] Chain letters always attempt to play on the irrational wishes or fears of their recipients – and often they succeed.[38] Most chain letters are forwarded to multiple recipients by friends or family members who appear to believe that they are avoiding some harmful situation or consequence by forwarding the e-mail.[39]

There are differing opinions as to when the first chain letter e-mail was actually sent. Some say it was sent as far back as 1971, even though it was a non-network one.[40] Others are of the view that the first e-mail chain letter was recorded in February 1982 which was a prayer of good luck by one Mark Bogg.[41] This was soon followed by other chain letters.[42] In 1994 the first "giant" spam incident reported was referred to as the "Jesus Spam".[43] This spam message drew attention because "it was apparently the first to be overtly abusive of mail and news systems using automated software to mail lists".[44] Below is an outline of different types of chain letters.

[37] The first fully-fledged chain letter is recorded as having been sent in 1888 by Daniel W. VanArsdale. Emery 'What is a chain letter?' supra n 35; also Snopes.com 'Chain linked' supra n 33; and Spamlaws.com 'The purpose of chain letter scams' http://www.spamlaws.com/chain-letter-scam-purpose.html (date of use: 5 November 2015).

[38] Examples of playing on recipients' irrational wishes or fears include, among others, sympathy chain letters which have proven in many instances to be hoaxes. Fear in this instance stems from the threats accompanying these letters that if the recipient fails to forward them, something bad will happen to them or their loved ones. See Emery 'What is a chain letter?' supra n 35.

[39] Other chain letters are sent to share content (which might be of an educational nature or at times inspiring). See Poteet *Canning Spam* 29-38.

[40] The 1971 spam was said to have been sent by a Tom Van Vleck, a co-author of the Compatible Time Sharing Systems (CTSS). He sent everybody on the CTSS mail a message on anti-war that stated: "THERE IS NO WAY TO PEACE, PEACE IS THE WAY". Apparently the sender defended it by saying "but this is important". See Templeton B 'Origin of the term "spam" to mean net abuse' http://www.templetons.com/brad/spamterm.html (date of use: 5 November 2015); also Zdziarski *Ending Spam* 7.

[41] Apparently the original copy was from the Netherlands, and it encouraged recipients to read and forward to others within 96 hours and that the chain should not be broken. Id Zdziarski 8.

[42] In 1988 a student struggling financially sent messages to several newsgroups with each post cross-posted to four or five newsgroups asking for financial assistance. This spam e-mail is referred to as the Jay Jay's College Fund and is regarded as the first charitable spam. Id Zdziarski 7; and Lynch 'Timeline of spam related terms and concepts' supra n 27.

[43] This spam message was the first major User's Network (USENET) spam on 18 January 1994. It was titled: "Global Alert for All: Jesus is Coming Soon". Id Zdziarski 9-10. USENET is a "collection of newsgroups where users can post messages and those posted messages are distributed via Usenet servers". See Usenet.org 'What is Usenet?' http://www.usenet.org (date of use: 3 March 2016).

[44] Ibid Zdziarski; also Templeton B 'Origin of the term "spam" to mean net abuse' http://www.templetons.com/brad/spamterm.html (date of use: 5 November 2015).

(i) Hoaxes

A hoax is an act intended to deceive recipients into believing that the information provided is correct, and that one needs to forward that information to as many people as possible.[45] There are different types of hoax e-mails circulating on the Internet today many of which warn users against viruses and/or "worms".[46] Other hoaxes include: sympathy hoaxes,[47] charity hoaxes,[48] bad-advice e-mails, and misleading recommendations,[49] bogus warnings or false-alert hoaxes, celebrity e-mail hoaxes, among others.[50] Perhaps the best-known hoax is the "Bill Gates hoax" which promised to give away hundreds of dollars to those who forwarded the e-mail message to a number of specified people.[51]

[45] See Schryen *Anti-spam Measures* 19; also Fleming & O'Carroll 'The art of the hoax' (2010) 16/4 *Parallax* 46; and Hitchcock *Net Crimes* 61. For reasons why these hoaxes get started see Hoax-Slayer 'Why do people create e-mail hoaxes' http://www.hoax-slayer.com/why-hoaxes.html (date of use: 5 November 2015).

[46] A "worm" is "similar to a virus by design and is considered to be a sub-class of a virus. Worms spread from computer to computer, but unlike viruses, they have the capability of travelling without any human action. Worms take advantage of files or information transport features on ones' system, which is what allows them to travel unaided. The biggest danger with worms is their capacity to replicate themselves on one's system, rather than one's computer sending out a single worm, it could send out hundreds or thousands of copies replicating itself, creating a huge devastating effect". Webopedia 'The difference between a computer virus, worm and Trojan horse' http://www.webopedia.com/DidYouKnow/Internet/2004/virus.asp (date of use: 5 November 2015); and Poteet supra n 39 64 and 89.

[47] The following are the most popular sympathy hoaxes: the Craig Shergold hoax which started in the 1980s concerning a 9 year old boy with a tumour. The boy apparently asked to receive enough get-well cards to break the Guinness record; another hoax was that of Jessica Mydek, a young girl dying of a rare form of cancer. Donations were solicited for that cause. This hoax implicated the American Cancer Society, which debunked it as unsubstantiated on their web site. See Howe W 'Sympathy hoaxes and warm fuzzy stories' http://www.walthowe.com/navnet/legends/sympathylegends.html (date of use: 5 November 2015); and American Cancer Society 'Rumors, myths and truths' http://www.cancer.org/AboutUs/HowweHelpYou/rumours-myths-and-truths (date of use: 5 November 2015).

[48] These hoaxes include: the Amy Bruce hoax; Walmart fire charity; boy shot by step dad charity; et cetera. See Hoax-Slayer 'Sick baby hoaxes-charity hoaxes' http://www.hoax-slayer.com/charity-hoaxes.html for the stories behind these hoaxes (date of use: 5 November 2015).

[49] Examples include: how to survive heart attack when alone; is lemon a cancer killer that is 10000 times stronger than chemotherapy et cetera. Hoax-Slayer 'Bad advice messages: Misleading recommendations' http://www.hoax-slayer.com/bad-advice-emails.html (date of use: 5 November 2015).

[50] Hoax Busters 'The big list of Internet hoaxes' http://www.hoaxbusters.org/#C (date of use: 5 November 2015).

[51] This was apparently done by e-mail tracking. See Snopes.com 'Thousand dollar bill' http://www.snopes.com/inboxer/nothing/billgate.asp (date of use: 5 November 2015).

(ii) Urban legends

An urban legend is an unverifiable story that has achieved wide circulation and deals with "outlandish, humorous, frightening, or supernatural events".[52] In some instances, the stories are based on actual occurrences that have been exaggerated or distorted in their retelling.[53] Other urban legends have their origin in people misinterpreting or misunderstanding stories that they have heard or read in the media, or have heard from actual witnesses of an event.[54]

Urban legends keep evolving by re-inventing and updating themselves, as was recently observed with the "Blood Gang legend",[55] which has evolved from anecdotal information to being shared via social media[56] and now Whatsapp.[57] Members of the public have been offered guidelines on how to detect urban legends and also to be cautious of messages that have particular characteristics.[58]

[52] Urban legends are "a kind of folklore consisting of stories often thought to be factual by those circulating them. They appear mysteriously and spread spontaneously in various forms and are usually false". Encyclopedia of the Unusual and Unexplained 'Superstitions, strange customs, taboos, and urban legends' http://www.unexplainedstuff.com/Superstitions-Strange-Customs-Taboos-and-Urban-Legends/index.html (date of use: 5 November 2015).

[53] Ibid*.*

[54] Hitchcock supra n 45 61-76 for a discussion on urban legends.

[55] This legend started doing the rounds as far back as the 1980s in the USA. The legend warns motorists about the danger of flashing at any car with no lights on at night. It goes on to say a new gang member might be under initiation and anyone who flashes their lights at that car will be a target (to be shot at and killed, in order for that initiate to complete the initiation requirements). See Snopes.com 'Lights out' http://www.snopes.com/crimes/gangs/lightsout.asp (date of use: 5 November 2015).

[56] In 2008 the same legend was being circulated warning South Africans to be on the lookout for the trend. The company that circulated this legend later stated that the message was sent in error and that it was to be ignored. At the time of writing the same legend is still doing the rounds. See IOL News 'Crime: Separating the fact from fiction' http://www.iol.co.za/news/south-africa/crime-seperating-the-fact-from-fiction-1.411773#.VlMSl3YrJhE (date of use: 6 November 2015).

[57] The term "WhatsApp" comes from the greeting "whats up". WhatsApp messenger is "a cross platform instant messaging application available to only smart phones like iPhones, Blackberry, et cetera. In addition to normal texting, WhatsApp messenger users can send each other images, videos and audio media messages as well as engage in group conversations between multiple users". Abbreviations 'What does WhatsApp stand for?' http://www.abbreviations.com/whatsapp (date of use: 6 November 2015).

[58] These guidelines include, but are not limited to the following characteristics: "a closing paragraph typed in capital letters and ending in multiple exclamation marks; the story begins with the affirmation that it is true and that it has happened to a friend, which is probably not an account of an actual event; the story received is similar to a story from several different sources, but with different names and details; there is no real evidence to support the story or its allegations; and the

(iii) Viruses

A virus is "a malicious code that masquerades as a file sent through e-mail attachments".[59] Viruses can send themselves to a number of e-mail addresses in the user's inbox inviting him or her to read an attachment.[60] When the virus attaches itself to a host file, it can render the file unusable.[61] Viruses ride on the back of files stored on a disk or in the boot-area of a floppy disk, and replicate when the disc is inserted into a computer.[62] Viruses were first written in the 1980s and can be destroyed through the reformatting of the hard disk, because like any other programme, they too will be wiped out.[63] However, if a virus has inadvertedly been copied to a disk and that disk is then inserted into another computer, it can re-infect the recipient computer although the original copy of the virus would have been destroyed on the host computer.[64]

Some viruses are used to do the following: distribute malware;[65] perform harmful functions which are sometimes referred to as payload, or a "bomb";[66] and also to turn

story describes some horrible crime perpetrated against an innocent victim". See Encyclopedia of the Unusual and Unexplained 'Superstitions, strange customs, taboos, and urban legends' http://www.unexplainedstuff.com/Superstitions-Strange-Customs-Taboos-and-Urban-Legends/index.html (date of use: 6 November 2015).

[59] Viruses have also been seen to "attach themselves to programs or files which enable them to spread from one computer to another, leaving infections as they travel. Viruses range in severity; some may cause only mild annoying effects, while others have the potential to damage hardware, software or files". Webopedia 'The difference between a computer virus, worm and Trojan horse' http://www.webopedia.com/DidYouKnow/Internet/2004/virus.asp (date of use: 6 November 2015); also Poteet supra n 39 64-6 and 88; Walker *Absolute Beginners Guide* 11; and Hitchcock supra n 45 341.

[60] Id Poteet 81-2.

[61] Id 66 and 88; also Walker supra n 59 11-18; and Hitchcock supra n 45 340-1.

[62] Id Walker 10; id Hitchcock 339-41 for different kinds of viruses.

[63] Poteet supra n 39 66; and ibid Walker. Walker notes that "while these viruses were written in the 1980s, they posed no great threat until the 1990s when those who owned personal computers started connecting to the Internet".

[64] Ibid.

[65] "Malicious software" or "malware" is "software designed to infiltrate or damage a computer system. This type of software is often sent as an unsuspicious e-mail attachment which installs itself when the user opens the file". See TechTarget 'Malware (malicious software)' http://searchsecurity.techtarget.com/definition/malware (date of use: 6 November 2015); Schryen supra n 45 21. In 2013 it was reported that malware was targeting user information like logins, passwords, and financial information. Alfreds D 'Spam declines, malware jumps: Kaspersky' http://www.news24.com/Technology/News/Spam-declines-malware-jumps-Kaspersky-20131119 (date of use: 6 November 2015).

[66] Walker supra n 59 13. Walker notes that "viruses share the following characteristics: they falsely claim to describe an extremely dangerous virus; they use pseudo-technical language to make

the systems they infect into “zombies”,[67] controlled by the virus authors in order to distribute more viruses.[68]

Petitions

A petition is a formally drafted request addressed to authorities and often bearing the names of the people who are making the request.[69] Electronic petitions (e-petitions) have been an Internet’s phenomenon since the 2000s.[70] They offer “instant comfort to those outraged by the latest ills in the world through their implicit assurance that by affixing their names to a statement decrying a situation and demanding change, the respondents will make a difference”.[71] These petitions do not as a rule contain information about the person they are intended to reach, and even if the intended recipient is clearly identified, the intended recipient(s) do not come with a guarantee that the person who is supposed to receive the document is in any position to influence matters.[72] No matter how well thought out these petitions might be, problems often arise, notably the lack of a guarantee that anyone collecting and collating the signatures will deliver the completed documents to the correct parties.[73]

perceived but impossible claims; they falsely claim that the report was issued or confirmed by a well-known company; and the recipient is aksed to forward the message to all their friends and colleagues”.

[67] A “zombie” is “a computer that has been implanted with a daemon that puts it under the control of a malicious hacker without the knowledge of the computer owner”. Webopedia ‘Zombie’ http://www.webopedia.com/TERM/Z/zombie.html (date of use: 6 November 2015).

[68] Rimmer SW ‘Death of spam: A guide to dealing with unwanted e-mail’ http://www.mindworkshop.com/nospam.html (date of use: 6 November 2015). Poteet supra n 39 69, provides the following checklist to protect computers which are infected by viruses: “one is advised not to open the attachment sent; run anti-virus software; and also run the latest patches on ones operating system and applications”.

[69] Dictionary.com ‘Petition’ http://www.dictionary.reference.com/browse/petition (date of use: 6 November 2015).

[70] Ibid.

[71] Lindner & Riehm (2009) 1/1 *JeDEM* 1 http://www.itas.kit.edu/pub/v/2009/liri09a.pdf (date of use: 6 November 2015); also GoPetition ‘Petitions at GoPetition’ http://www.gopetition.com/petitions (date of use: 6 November 2015).

[72] In the absence of identifying details such as physical addresses and phone numbers, the names listed on petitions are unverifiable and easily falsified. See Lindner & Riehm supra n 71 3.

[73] GoPetition ‘Petitions at GoPetition’ http://www.gopetition.com/petitions (date of use: 6 November 2015).

The mere existence of a petition also does not ensure that anyone will do anything with it once it has been completed.[74] However, some e-petitions have made an impact that saw government officials and the public weighing in on the contents of the petition.[75] A further problem with e-petitions is that there is no assurance that the signatures are indeed those of different people and have not been generated by a single individual.[76] Apparently it takes little by way of programming skills to create a sequence of code that will randomly generate fake names, e-mail addresses, and cities (or whatever combination these e-petition requires).[77] E-petitions can also be characterised as formal[78] or informal.[79]

Other non-commercial spam e-mail includes political e-mails.[80] The non-commercial spam e-mails above will however, not qualify as spam in anti-spam laws as they lack the commercial component in them.[81] The discussion on commercial spam e-mails follows below.

[74] Ibid. A case in point where a petition reached its destination but the matter could not be resolved, involved a campaign by white South Africans concerned about racism and crime. The group launched a Facebook petition to return to Holland (where their ancestors lived 300 years ago). This petition reached the intended recipients but the contents of the petition was declined, as one Dutch official stated that "chances of receiving Dutch citizenship are almost non-existent". The Christian Science Monitor 'White South Africans use Facebook in campaign to return to Holland' http://www.csmonitor.com/World/Africa/2010/0517/white-South-Africans-use-Facebook-in-campaign-to-return-to-Holland (date of use: 5 November 2015).

[75] See in particular the e-petition titled 'Stop racism at Pretoria Girls High' calling out the school's management to ensure that its code of conduct did not discriminate against Black and Muslim girls. This petition was said to have gathered more than 10 000 signatures within three days of its creation. See the Guardian 'Racism row over South Africa school's alleged hair policy' https://www.theguardian.com/world/2016/aug/29/south-africa-pretoria-high-school-for-girls-afros (date of use: 1 September 2016).

[76] Snopes.com 'Petitions' http://www.snopes.com/inboxer/petition/internet.asp (date of use: 5 November 2015).

[77] Ibid.

[78] See Lindner & Riehm supra n 71 3. Lindner and Riehm notes that a formal e-petition refers to "institutionalised and at least to some extent legally codified e-petition system operated by public institutions".

[79] Ibid Lidner & Riehm. Informal e-petitions are "systems established and managed by non-governmental, private organisations. Informal e-petitions usually seek to address public institutions after a certain number of signatures have been collected. The two types of informal e-petition are noted as: e-petitions initiated by NGOs as part of political campaigns; and e-petition platforms operated by private organisations (both commercial and not-for-profit) which provide the Internet-based infrastructure to initiate e-petitions and collect signatures online".

[80] For the problems caused by political spam and whether this kind of spam should be regulated or not see: Grossman (2004) 19/4 *Berkeley Technology Law Journal* 1533 ff.

[81] See Buys 'Online consumer protection and spam' 160.

(b) Commercial spam e-mails

Unlike the annoying spam e-mails above, commercial e-mails are the most enticing resulting in uninformed consumers assuming that the benefits offered by these e-mails are real. These are also the most dangerous e-mails which claim to offer free gift vouchers and also money from inheritances. The following are examples of commercial spam messages.

The DEC spam

The first form of electronic advertising is thought to have been distributed on a wide area network in 1978 as an advertisement from Digital Equipment Corporation (DEC).[82] DEC sent an invitation to all ARPAnet addresses on the USA west coast inviting recipients to come and view DEC's newest decsystem-20 family of computers. The e-mail addresses of all recipients of the advertisements had to be manually typed and sent by DEC through its marketing department.[83] Apparently this created a significant overload on what was then considered low-bandwidth lines (the equivalent of today's dial-up system).[84]

The Green Card Lottery spam

The most talked about spam in 1994 was the Canter and Siegel spam referred to as the "Green Card Lottery Spam".[85] This husband and wife lawyer team sold green card lottery tickets to immigrants by sending messages to newsgroups advertising their services. The reaction was negative and recipients started sending e-mails to the

[82] Zdziarski supra 40 4; and also Templeton B 'Reaction to the DEC spam of 1978' http://www.templetons.com/brad/spamreact.html (date of use: 5 November 2015)

[83] Id Zdziarski 4-7.

[84] Id 5-6.

[85] Id 10-13; also Singel R 'April 12, 1994: Immigration lawyers invent commercial spam' https://www.wired.com/2010/04/0412canter-siegel-usenet-spam (date of use: 6 November 2015). Singer notes that Canter and Siegel profited from this spam, and that they also tried to cash in on their popularity by writing a book titled: "How to make a fortune on the information superhighway", which was apparently a flop. Canter was subsequently disbarred in 1997 by the state of Tennessee in part for apparently spamming.

couples' mailboxes in retaliation. This spam gave birth to the first known "bulk mailer software".[86]

Scams

Perhaps the most dangerous spam e-mails that one can receive are scam e-mails. A scam is defined as a dishonest attempt to trap the recipient into parting with money.[87] Jayamala note that a scam is "generally sent personally (or electronically) by a scammer with persuasive techniques that can be difficult to resist".[88] In the 1990s a number of "make money fast" postings on the Internet emerged, but were usually once-off postings each from different individuals.[89] These scams come in a variety of forms including, but not limited to, Ponzi schemes, pyramid schemes, Nigerian 419 schemes, and most recently, phishing scams.[90] These various scams are discussed individually in what follows.

(i) Ponzi and pyramid schemes

A Ponzi scheme is "an investment fraud that involves the payment of purported returns to existing investors from funds contributed by new investors".[91] A Ponzi scheme differs

[86] See Fuqua J 'Why lawyers have a bad name: A net legend' http://www.jamesfuqua.com/lawyers/jokers/canter.shtml (date of use: 6 November 2015). Bulkmail is e-mail sent to a large number of people for marketing purposes. WiseGeek 'What is bulk email?' http://www.wisegeek.com/what-is-bulk-email.htm (date of use: 10 November 2015).

[87] It is also defined as a fraudulent or deceptive act or operation. Merriam Webster 'Scam' http://www.merriam-webster.com/dictionary/scam (date of use: 6 November 2015).

[88] See Jayamala (2014) 95/1131 *Australian Journal of Pharmacy* 18-19 http://search.informit.com.au/fullText;dn=759638788394502;res=IELHEA (date of use: 6 November 2015).

[89] Templeton 'Origin of the term 'spam' to mean net abuse' supra n 40; and Lynch 'Timeline of spam related terms and concepts' supra n 27.

[90] Other types of scam include: disaster relief schemes; credit card scams; food scams; work at home plans; lottery scams; and identity fraud scams. See Scambusters.org 'Internet scams, identity theft, and urban legends: are you at risk?' http://www.scambusters.org (date of use: 6 November 2015); also Nedbank 'Scams' http://www.nedbank.co.za/website/content/crimeawareness/scams.asp (date of use: 6 November 2015).

[91] Investopedia 'Ponzi scheme' http://www.investopedia.com/terms/p/ponzischeme.asp (date of use: 6 November 2015). This scheme is named after Charles Ponzi who deceived thousands of New England residents into investing in a postage stamp speculation scheme back in the 1920s. The Museum of Hoaxes 'Charles Ponzi and the Ponzi scheme' http://hoaxes.org/archive/permalink/charles_ponzi_and_the_ponzi_scheme (date of use: 6 November 2015).

from a pyramid scheme in that one person takes money from other individuals as an "investment" but does not necessarily tell them how their returns will be generated.[92] The organiser of the Ponzi scheme often solicits new investors by promising to invest funds in opportunities claimed to generate high returns with little or no risk.[93] In many Ponzi schemes the fraudsters focus on attracting additional money to make promised payments to earlier-stage investors, and also use that money for personal expenses instead of engaging in any legitimate investment activity.[94] In South Africa thousands of individuals, are reported to have lost hundreds of millions of Rand to these Ponzi schemes.[95] Characteristics of Ponzi schemes are brought to people's attention so they can protect themselves from falling prey to these types of scam.[96]

A pyramid scheme on the other hand is a scheme structured like a pyramid in which participants attempt to make money by recruiting new participants into the program.[97] This scheme starts with one person who recruits another person, who is then required to 'invest' a certain amount (for example, R 1 000) which is paid to the initial recruiter.[98] In order for the first person to make their money back, the new recruit must then

[92] Investopedia 'What is a pyramid scheme' http://www.investopedia.com/articles/04/042104.asp (date of use: 6 November 2015).

[93] Modern-day Ponzi schemes include the infamous Benny Madoff (in the USA) who is currently serving 150 years in prison for orchestrating a multi-billion dollar Ponzi scheme which swindled money from thousands of investors, some of them prominent figures in Hollywood such as Stephen Spielberg et cetera. See US Securities and Exchange Commission 'Ponzi schemes' http://www.sec.gov/answers/ponzi.htm (date of use: 6 November 2015).

[94] Ibid.

[95] See in particular the Defencex Ponzi scheme. This scheme supposedly targeted South Africa's wealthiest families. According to the report this scheme was perpetrated by Net Income Solutions known as Defencex. The company swindled R800m from 195 000 members before its bank account was frozen by the High Court (Cape Town) in February 2013. See: SouthAfrica.info 'Ponzi scheme money frozen' http://www.southafrica.info/news/business/ 690383.htm (date of use: 6 November 2015); and Volker (2011-2012) *Auditing SA* 5-10 for a discussion and schematic illustration of a Ponzi scheme.

[96] US Securities and Exchange Commission 'Ponzi schemes' http://www.sec.gov/answers/ponzi.htm for the characteristics of Ponzi schemes which include, among others: overly consistent returns; and unregistered investments. See also Reese M 'Warning signs of ponzi schemes: part 2' http://www.moneyweb.co.za/archive/part-2-warnings-signs-of-ponzipyramid-schemes (date of use: 6 November 2015).

[97] US Securities and Exchange Commission 'Pyramid schemes' http://www.sec.gov/ answers/pyramid.htm (date of use: 5 November 2015); also Reese M 'Warning signs of ponzi schemes: part 2' http://www.moneyweb.co.za/archive/part-2-warnings-signs-of-ponzipyramid-schemes (date of use: 6 November 2015).

[98] Investopedia 'What is a pyramid scheme' http://www.investopedia.com/articles04/042104.asp (date of use: 6 November 2015); also Rothchild (1999) 74/3 *Indiana Law Journal* 907.

introduce more people who in turn will make the R 1 000 contribution.[99] These schemes promise sky-high returns over a short period merely for handing over money and getting others to do the same.[100] The scammers behind these schemes may also go so far as to making the program resemble a multi-level marketing program.[101] But despite their claims to have legitimate products or services to sell, these scammers simply use money coming in from new recruits to pay off early-stage investors.[102] The object is that as more people are added the earlier ones will move higher up the pyramid, one tier at a time, until ultimately they reach the top spot.[103] The South African Reserve Bank launched an anti-pyramid scheme campaign in a bid to educate citizens on how to spot and avoid pyramid schemes.[104]

(ii) Nigerian 419 scam

The Nigerian scam, otherwise known as the 419 scam, apparently started circulating in the 2000s on the Internet.[105] These scam messages are sent via e-mail generally to a number of persons, claiming that the recipients assistance is needed to access a large sum of money, which in most cases does not exist.[106] The scams are historically said to be "a modern derivation of traditional centuries of West African scams and pranks, such

[99] Ibid Investopedia.

[100] Ibid.

[101] US Securities and Exchange Commission 'Pyramid schemes' supra n 97; and Rimmer 'Death of spam: A guide to dealing with unwanted e-mail' supra n 68. A multi-level marketing scheme is "a scheme where a person is recruited to sell products or services that actually have some inherent value. As a recruit, one can make profit from the sales of the product or services, so they won't necessarily have to recruit more people to sell those products or services".

[102] Ibid US Securities and Exchange Commission 'Pyramid schemes' supra n 97.

[103] Corbett J 'Reserve Bank launches anti-pyramid scheme campaign' http://www.moneyweb.co.za/reserve-bank-launches-antipyramid-scheme-campaign (date of use: 6 November 2015).

[104] Ibid.

[105] See Ampratwum (2009) 16/1 *Journal of Financial Crime* 68 for historical perspective; and Lynch 'Timeline of spam related terms and concepts' supra n 27. Ampratwum notes that "the Nigerian scam is named after a formerly relevant section of the Criminal Code of Nigeria. These scams are believed to have been in circulation since the 1980s under the Successive Governments of Nigeria. In these scams a target receives unsolicited e-mail letter concerning Nigerian money laundering, or illegal proposal".

[106] Ibid Ampratwum.

as the “Red Mercury” scam, sent by fax or letter”.[107] Although these scams are set to have originated in Nigeria and are termed “Nigerian scams”, they are set to be sent from countries other than Nigeria.[108] Scammers in the Nigerian 419 scam normally solicit help from others by promising to deposit exorbitant amounts of money into those recipients bank accounts.[109] Initially these scams targeted those in business, but they have now expanded to include average citizens “due to the low cost of e-mail transmission in relation to potential gains”.[110] The money can be from a number of sources,[111] and the sums transferred are on average apparently in the hundreds of thousands, even millions, of dollars and the recipient is usually promised a commission for assisting in the transfer.[112] Senders of these messages often claim to be government officials (from a Department in one of the Ministries, such as an auditing bureau, et cetera), Nigerian royalty, a spouse of the deceased, a relative, aide, or confidante of a deposed leader, or a religious figure such as Deacon, Brother, or Pastor.[113] Atta-Asamoah[114] is of the opinion that these scams can be broken down into three stages, namely:

(a) Stage 1: scouting and harvesting. This stage involves searching and extracting e-mail addresses and making contact with the targets;
(b) Stage 2: relationship building and profiling. In this stage the scammers attempt to build a relationship with the target ranging from friendship and business social relationship. As the relationship deepens through frequent communication, the scammer profiles the target. This stage requires great tact and care to avoid the victim from becoming suspicious; and
(c) Stage 3: operational stage. The scammer proposes an idea involving the transfer of money or goods. Experienced scammers proceed cautiously at this stage since any wrong or suspicious move could strain the relationship and allow the target to escape.

[107] The Red Mercury scam is “a magical substance advance fee fraud scam very similar to Black Currency 419”. See Atta-Asamoah (2009) 18/4 *African Security Review* 107.

[108] Other countries include Ghana, Cameroon, Sierra Leone, and any other foreign countries. Ibid; and Ampratwum supra n 105 68.

[109] Smith (2009) 23/1 *Cultural Studies* 27-47 for a discussion of these scams; also Kassner M ‘The truth behind those Nigerian 419 scammers’ http://www.techrepublic.com/blog/it-security/the-truth-behind-those-Nigerian-419-scammers (date of use: 6 November 2015); and Glickman (2005) 39/3 *Canadian Journal of African Studies* 463-8.

[110] Nigerian scams ‘West Africa scam/Nigeria advance fee fraud in Internet web mail frauds and email letter scam’ http://www.crimes-of-persuasion.com/Crimes/Business/nigerian.htm (date of use: 6 November 2015).

[111] Ibid. These sources include: the transfer of funds from over invoiced contracts; sale of crude oil at below market prices; disbursement of money from wills; contract fraud (COD of goods or services); purchase of real estate; or conversion of hard currency or even an inheritance.

[112] Ibid.

[113] Ibid. Also Smith supra n 109 27-47.

[114] See Atta-Asamoah supra n 107 109-12.

The Nigerian 419 scam is considered "the most dangerous and in some cases has "apparently" resulted in the death of individuals who were lured into travelling to Nigeria to claim their fortune, only to be held to ransom on arrival so as to extract money from their loved ones".[115] Countries have issued alerts to their citizens who might be involved in or affected by such scams to file complaints with the Nigerian Embassy or High Commission in their respective countries.[116] South Africa has additional specific instructions[117] regarding the 419 scams which include providing assistance to individuals in avoiding these scams.[118] In order to detect scam messages, members of the public are advised to be on the lookout for certain characteristics in these scam letters.[119] The latest version of the 419 scam is the "419 heartbreaker scam".[120]

[115] Nigerian scams 'West Africa scam/Nigeria advance fee fraud in Internet web mail frauds and email letter scam' supra n 110; and Rimmer 'Death of spam: A guide to dealing with unwanted e-mail' supra n 68.

[116] Nigeria: The 419 Coalition Web site 'The Nigerian scam (419 advance Fee fraud) Defined' http://home.rica.net/alphae/419coal/ (date of use: 5 November 2015).

[117] These additional instructions include "faxing all scam documents referencing South Africa, especially those with phone numbers or banking information of a commercial branch, to the South African Police Service. Phone numbers and contact details where the documents need to be sent are provided – eg, fax and e-mail addresses". The following rules are also provided for doing business with Nigeria regarding the 419 scam: "never pay anything up front for ANY reason; never extend credit for any reason; never do anything until their cheque clears; never accept any help from the Nigerian Government; and never rely on your Government to bail you out". See Glickman (2005) *Canadian Journal of African Studies* 463-70; also Ampratwum supra n 105 68-70; Nigerian: The 419 Coalition Web site 'The Nigerian scam (419 advance Fee fraud) Defined' supra n 116.

[118] The following are pointers for users: "protect ones' personal information. Share credit or personal information only when buying from a company you know and trust; know the people one is dealing with. One should not do business with any company that will not provide its name, street address, and telephone number; one should take time to resist any urge to 'act immediately' despite the offer and the terms. Once the money is turned over to the scammer one may never get it back; read the small print, get all promises in writing, and review them carefully before making a payment or signing a contract; and never pay for a "free" gift. Disregard any offer that asks one to pay for a gift or prize: if it's free or a gift, one should not have to pay for it". See OnGuardOnilne.gov 'Spam' http://www.onguardonline.gov/spam.html (date of use: 6 November 2015).

[119] The characteristics are as follows: "many scammed e-mail are addressed to "presidents" or "CEOs" rather than a specific name (nowadays Madam or Sir); e-mails may contain spelling mistakes and grammatical errors which give the reader a sense of intellectual superiority, sympathy, or assurance of origin; they are almost always written in capital letters reminiscent of older type writers even though currently e-mailed; the amounts to be transferred invariably in the tens of millions of dollars, is also written out in text form, that is, $40 000 000 (forty million United States Dollars); and the e-mail states that the recipients have been recommended or their honesty and business acumen has been verified". See Nigerian scams 'West Africa scam/Nigeria advance fee fraud in Internet web mail frauds and email letter scam' supra n 110.

[120] This latest version targets online dating sites. See Kruger H 'The Top 10 Scam types in South Africa' http://www.junkmail.co.za/blog/the-top-10-scam-types-in-south-sfrica/6897 (date of use: 6 November 2015).

(iii) Phishing

Phishing is "the act of sending an e-mail or SMS[121] to a user falsely claiming to be an established legitimate enterprise (in most cases a banking institution) in an attempt to scam users into surrendering private information which will be used for identity theft".[122] These users are lured to bogus web sites, which appear legitimate, and would then require users to perform normal log in procedures.[123] Once this has been done, the scammers obtain personal information such as bank account numbers and online banking passwords.[124] The most infamous phishing scams in South Africa have been the South African Revenue Service (SARS) e-filing tax return scam, and those that involve banking institutions.[125] These scams have been debunked by these respective enterprises.[126] In addition to the above, the following scams were reported as plaguing South Africa: false payment confirmations; unethical app download charges; SIM swops; credit card skimming; and the Microsoft scam, to name but a few.[127] While consumers are exposed to these deceptive practices, spammers and scammers have turned those activities into a lucrative business so exacerbating the problem.

2.4 Lucrative business for spammers

[121] Phishing send via SMS is called "smishing" and it is similar to phishing but refers to fraudulent messages sent by SMS or text message. TechTerms 'Smishing' http://www.techterms.com/definition/smishing (date of use: 6 November 2015); also Kennedy (2009) Aug/Sept *Journal of Marketing* 22; Molefi N 'Consumers ripped off by spam SMSes' http://www.sabc.co.za/news/a/ce063b8041dfe949a29eaf1c2eddf908/Consumers-ripped-off-by-spam-SMSes-20131811 (date of use: 6 November 2015); and Cloudmark 'Spammers target mobile users with more than 350,000 unique SMS spam variants in 2012' http://www.cloudmark.com/en/press/spammers-target-mobile-users-with-more-than-350-000-unique-sms-spam-variants-in-2012 (date of use: 6 November 2015).

[122] Webopedia 'Phishing' http://www.webopedia.com/TERM/P/phishing.html (date of use: 6 November 2015). For a discussion on phishing see generally Cassim (2014) 47 *CILSA* 401 ff.

[123] Ibid Cassim.

[124] Ibid.

[125] SARS 'Scams and phishing attacks' http://www.sars.gov.za/TargTaxCrime/Pages/Scams-and-Phishing.aspx?k=SARSScamSource%3Aemail (date of use: 6 November 2015); also ABSA 'Phishing scams' http://www.absa.co.za/Absacoza/Security-Centre/Scams/Phishing-Scams (date of use: 6 November 2015); and Cassim supra n 122 412-16 for a South African perspective on this problem.

[126] Ibid SARS 'Scams and phishing attacks' and ABSA 'Phishing scams'.

[127] Kruger 'The Top 10 Scam types in South Africa' supra n 120.

Given the above, it is no surprise that spam has become the scourge it is today. It is noted how spammers and scammers swindle money out of unsuspecting individuals. This they do by extracting those individuals personal information for purposes of "spamming" them on a large scale. This shows how spammers have managed always to stay one step ahead of their victims, becoming more aggressive through the years and even profiting from their deceptive practices. It is noted that spammers started using different programmes – such as spamvertise[128] and spamware[129] – to distribute their spam e-mails during the 1990s.[130]

In that decade the act of spamming became entrepreneurial, and spammers, built businesses through flooding recipients' mailboxes. Examples of such spammers include: Jeff Slaton dubbed the "Spam King" who made spam appear lucrative, by claiming "to have made $42 per distribution of between fifteen and thirty e-mails weekly".[131] Krazy Kevin Lipsitz also began a notorious newsgroup-spamming campaign, specialising in various spam promotions.[132] Around the same time Velveeta was also sending cross-posting articles to a number of newsgroups.[133] Sanford Wallace otherwise known as "Spamford" also began "a one man spam campaign" and later founded Cyber Promotions (aka CyberPromo, a notorious spam outfit).[134] Recently

[128] Spamvertise is defined as: "to advertise products and services via unsolicited bulk e-mail, or to abuse a particular Internet resource such as a domain name by spamming frequently contributing to a blacklisting or loss of value of the resource". Urban Dictionary 'Spamvertise' http://www.urbandictionary.com/define.php?term=spamvertise (date of use: 10 November 2015).

[129] Spamware is "software that is designed for sending spam in ways that hide the sender, attempting to circumvent spam filters, or which contains features only of use to spammers. Spamware is developed by criminals for criminals specifically for illegal use often containing features such as the ability to falsify e-mail headers to hide the true source of the spam". Spamhaus 'Spamware' http://www.spamhaus.org/whitepapers/spamware (date of use: 10 November 2015).

[130] Lynch 'Timeline of spam related terms and concepts' supra n 27.

[131] See Zdziarski supra n 40 14-15; also Wired 'Spam king' https://archive.wired.com/wired/archive/4.02/spam.king_pr.html (date of use: 10 November 2015); and Garfinkel S 'Spam King' https://www.wired.com/1996/02/spam-king (date of use: 6 November 2015).

[132] Id Zdiariski 15; also Lynch 'Timeline of spam related terms and concepts' supra n 27; and Rahul.net 'Overview of spam from Lipsitz' http://www.rahul.net/falk/Lip (date of use: 10 November 2015) for a sample of the spam sent by Lipsitz.

[133] Ibid Lynch 'Timeline of spam related terms and concepts' supra n 27.

[134] See Zdziarski supra n 40 15-16; ibid Lynch; ibid Wired 'Spam king'. Hormel Foods objected to Sanford Wallace's use of the word spam and registration of the web site "spamford", thus keeping spam (its brand name) from being used as synonymous for unwanted e-mail. The objection was later abandoned.

Wallace was indicted for spamming Facebook users.[135] Nowadays organisations such as Spamhaus monitor spammers that are notorius for their spamming activities, and by so doing alert stakeholders to be on the lookout for such characters so as to avoid falling prey to such deceptive practices.[136]

While some spammers were benefiting by selling books or using new programmes to send even more spam, others were collecting lists of e-mail addresses and selling them.[137] The sale of lists of e-mail addresses was recorded as a lucrative business as far back as the 1990s,[138] and has been escalating with each passing year.[139] While it is not clear how many lists are now up for sale, it is common cause that government departments, organisations, businesses et cetera, own large numbers of databases which they have been accused of selling to third parties.[140]

2.5 Conclusion

In this chapter, the development of spam in an online environment was highlighted. It was shown how spam started with just one message sent manualy in the 1970s, and has evolved into millions of spam e-mails clogging up mailboxes throughout the world on a daily basis. It is clear from the above that the problem has escalated and that those behind these scam and spam e-mails are benefitting from their deceptive practices. Newer modes of communication are also contributing to the scourge by shrinking

[135] The Register 'Spanking Spam King: Sanford Wallace faces jail for Facebook flood' http://theregister.co.uk/2015/08/25/spammer_wallace_faces_jail_facebook_scam (date of use: 10 November 2015); also The FBI (San Francisco Division) 'Sanford Wallace indicted for spamming Facebook users' https://www.fbi.gov/sanfrancisco/press-releases/2011/sanford-wallace-indicted-for sending spam messages to Facebook users (date of use: 10 November 2015).

[136] See Spamhaus 'The world's worst spammers' http://www.spamhause.org/statistics/spammers for a list of the world's worst spammers (date of use: 7 September 2015).

[137] Lynch 'Timeline of spam related terms and concepts' supra n 27.

[138] Ibid. Apparently in 1995 2 million e-mail addresses were offered for sale.

[139] Ibid. In 1996 it was reported that the lists offered for sale increased from 7 million to 11 million; followed by 31 million; 57 million; and 80 million in 1997; in 1998 those lists amounted to 91 million, and in 2001 to 209 million.

[140] Recently, one of South Africa's cell phone providers was accused of sharing its customers' personal information. The explanation provided by the cell phone giant was that there was a breach in their systems when it was upgraded. See Mochiko T 'Cyber security: oversharers anonymous' http://www.financialmail.co.za/features/2014/11/06/cyber-security-oversharers-anonymous (date of use: 10 November 2015).

boundaries and making recipients available around the clock. Direct marketers and spammers alike have wasted no time in making their presence felt in those mediums. While consumers are falling prey to these practices, spam is causing problems.

In the next chapter focus will be on the problems caused by spam and how spammers use certain methods to extract personal information of consumers for spam purposes.

CHAPTER 3

THE EFFECT OF SPAM ON E-MAIL MESSAGES

3.1 Introduction

In the previous chapter we observed how spam evolved from a nuisance to an all-out attack on e-mail boxes. We have also seen how spam is an effective marketing tool sometimes masked in deceptive activities such as scams. And while these spamming activities causes problems, spammers have in turn benefited from the whole exercise. The question then, is how do spammers and marketers alike get the personal information of individuals in order to send spam messages? This they do by extracting personal information of individuals from web sites. While the free exchange of personal information is set "to promote consumer welfare (by encouraging businesses to develop and market goods and services that most interest their existing and potential consumers), it also raises issues of fairness and confidentiality".[1]

In this chapter focus is on the effect of spam on e-mail messages. The following will be at the centre of the discussion: the methods that spammers use to obtain e-mail addresses; the problems caused by spam; and technical measures used to limit spam.

3.2 Methods used to extract e-mail addresses for purposes of spam

3.2.1 Background

Personal information is a broad term that encompasses characteristics of individuals including, but not limited to: their names; address; phone numbers; codes or symbols; and fingerprints.[2] An e-mail in this instance also falls within that definition because it identifies an individual in cyberspace. In order for a spammer to send unsolicited communications he or she must be in possession of lists of e-mail addresses of consumers to whom they wish to pitch their goods, products or communications. These

[1] Irving (1996) 1 *University of Chicago Legal Forum* 9; and De Bruin *Consumer Trust* 11.

[2] BusinessDictionary.com 'Personal information' http://www.businessdictionary.com/definition/personal-information.html (date of use: 10 November 2015).

e-mail addresses can be obtained in a variety of ways including by consumers themselves divulging the information voluntarily by filling out subscriptions to newsletters. It can also be collected while the individual is "surfing the Internet".[3] The following methods, each of which is discussed separately, are some of the most popular methods used to source consumers' e-mail addresses in order to send spam messages: online profiling and the use of cookies; spyware; dictionary attacks; using software to harvest e-mails addresses; and also spoofing.

3.2.2. Online profiling and the use of cookies

3.2.2.1 Online profiling

Most individuals do not realise that when they surf the Internet, they leave a trail of information on every web site they visit.[4] The trail – otherwise referred to as "mouse droppings"[5] – is valuable to online merchants who collect that information to be used for marketing purposes.[6] This trail of information reveals extensive personal information pertaining to those individuals, and in the wrong hands can be used to inflict harm to those individuals.[7] The information left behind during a web site visit is routinely collected without the individual's knowledge and used for a variety of purposes without the individual's consent.[8] This raises questions as to how businesses market their goods and services to consumers, and how a consumer's online shopping experience

[3] The phrase "surfing the Internet" or "surfing the net" is described as "an undirected type of browsing on the Internet without a planned search strategy or definitive objective". See Reference 'What does the phrase 'surf the Internet mean' https://www.reference.com/technology/phrase-surf-internet-mean-8bf3144adff725c (date of use: 3 March 2017).

[4] Irving supra n 1 7.

[5] Ibid. Mouse droppings are pixel(s) (usually single) that are not properly restored when the mouse pointer moves away from a particular location on the screen, producing an appearance that the mouse pointer has left droppings behind. Dictionary.com 'Mouse droppings' http://dictionary.reference.com/browse/mouse+droppings (date of use: 10 November 2015).

[6] Irving note that "while these droppings are beneficial to online merchants, to the user they are detrimental because their information might be sold to other online merchants who will in turn send spam in order to advertise their products or services. Several online companies already track and sell information derived from these mouse droppings". See Irving supra n 1 7; and Budnitz (1998) 49/4 *South Carolina Law Review* 851.

[7] Id Irving 7 and 9.

[8] Idler (1999) 138/7 *Trusts and Estates* 42; also Jordaan (2007) 3/1 *International Retail and Marketing Review* 42-53.

can be customised and personalised without leaving a trace.[9] Profiling starts when consumers enter a merchant's site irrespective of whether or not a purchase is made.[10] Consumers may visit a merchant's site several times before acting on an offer or buying goods and services.[11] There are a number of online profiling and personalisation systems available and each uses its own database, even though they all follow a basic outline.[12] In order for one to build an online profile database, one need to know what important information to request based on the knowledge of one's consumers.[13]

The purpose of collecting and analysing this data is to allow marketers to draw a variety of inferences about each consumer's interests and preferences.[14] These merchants are most often invisible to consumers and all the consumer sees are the web sites they visit.[15] This also enables computers to make split-second decisions about how to deliver ads directly targeted at the consumer's specific interests.[16] The result is a detailed profile that attempts to predict the individual consumer's tastes, needs, and purchasing habits.[17] Unless the web sites visited by consumers provide notice of the marketers' presence and the collection of data consumers will remain unaware that their activities are being monitored online.[18] Even when consumers are aware of this kind of profiling, they cannot effectively prevent it from happening, and there have, consequently, been calls for a need to regulate this form of harmful practice.[19]

[9] Suchet P 'Real time online profiling' http://www.clickz.com/clickz/column/1718804/real-time-online-profiling (date of use: 10 November 2015); and Steindel (2011) 17/2 *Michigan Telecommunications and Technology Law Review* 459-64 on how online profiling work.

[10] Bennett (2011) 44/4 *John Marshall Law Review* 899-904 on the origins of online behavioural advertising, and how that works; also Hoofnagle et al (2012) 6 *Harvard Law and Policy Review* 279-280 on how web tracking works.

[11] Ibid Bennett.

[12] See Kania D 'The art and science of online profiling' http://www.clickz.com/clickz/column/1702454/the-art-and-science-of-online-profiling (date of use: 10 November 2015).

[13] Ibid Kania; also Suchet 'Real time online profiling' supra n 9.

[14] Federal Trade Commission 'Online profiling: a report to Congress part 2 recommendations' http://www.steptoe.com/assets/attachments/934.pdf (date of use: 10 November 2015).

[15] Ibid.

[16] Suchet 'Real time online profiling' supra n 9.

[17] Ibid.

[18] Ibid.

[19] Steindel supra n 9 466-75; also Whipple (2013) 21 *LBJ Journal of Public Affairs* 90-100 where the author lists a number of regulatory tools including: self-regulatory initiatives; do-not-call lists; specialty consumer reporting agencies; and Bennett supra n 10 907-13.

3.2.2.2 Cookies

Online profiling is most effective when cookies are set on web sites to gather information about prospective buyers. A cookie is “a file that is downloaded to a user’s computer to remember the user’s preferences each time he or she returns to the site”.[20] Cookies are widely used by the marketing industry and are regarded by that industry as essential to the efficient operation of commercial web sites.[21] Cookies basically allow businesses to build a database of consumer habits and hobbies by recording where they created their shopping baskets and what items were in those baskets.[22] They also track where those consumers go online after they leave the web site(s).[23] This gathered information will be transfered to web servers.[24] The collection of information varies from cookie to cookie depending on the lifespan of the specific cookie.[25]

The cookie’s intended purpose is to eliminate the need for web users to re-enter username and password each time they want to read news articles or enter a web site requiring membership.[26] As part of a self-help solution consumer’s are advised to do the following to prevent cookies from being set on their computers: maintain a cookie file on their computers; set their browser to reject all or some cookies; receive an alert when cookies attempt to download themselves onto the consumer’s hard drive; install software that manages cookies on their behalf; and select an opt-out (if any) provided

[20] King (2003) 12 *Information and Communications Technology Law* 228; also Rogers (2004) 25 *Business Law Review* 293; Albrecht (2002-2003) 36 *Suffolk University Law Review* 422; and Lanois (2010) 9/2 *Northwestern Journal of Technology and Intellectual Property* 32-43 where the author discusses privacy in the digital world and the use of cookies.

[21] Ebersöhn (2004) 16/4 *SA Merc LJ* 741 ff; id King 229; ibid Rogers where the author notes that “cookies are potentially a silent, hidden, and unseen Trojan horse, although they may appear harmless and potentially necessary for the correct functioning of the web sites, they contain monitoring devices which track a person’s usage of the Internet, and this may be a threat to the privacy of the individual”; and Traung (2010) 31/10 *Business Law Review* 216-17.

[22] Youngblood (2001) 11/1 *DePaul-LCA Journal of Art and Entertainment Law* 48; and Buys ‘Privacy and the right to information’ 384-387.

[23] Ibid

[24] King supra n 20 228; and Lanois supra n 20 32-43.

[25] Ibid King; and Brandon (2012) 29 *John Marshall Journal of Computer and Information* 641-2.

[26] When one submits data online the following happens: the data is e-mailed to a designated e-mail box; the data is stored in a database; or some combinations of these options occur. See Leiserson (2002) 94 *Law Library Journal* 541 and 546.

by web site operators.[27] Most cookies are set to be entirely benign and, indeed, play an important role in web browsing and e-commerce.[28] In an effort to move away from standard cookies, newer tracking devices have also been identified.[29] Big data[30] is also used by marketers who are trying better to understand their customers and so hopefully improve relationships.[31] The phrase big data is used to describe "a massive volume of both structured and unstructured data that is difficult to process using traditional database and software because of its volume".[32] While big data assists businesses to thrive, it also puts consumers in the precarious situation of always having to try to protect their personal information.[33]

3.2.3 Harvesting e-mail addresses

Harvesting is defined as "the use of a program to scan through documents, e-mails, bulletin boards, and other material to identify and store e-mail addresses".[34] Most often harvested e-mail address lists are either created by marketers, compiled into a contact list and then sold.[35] These can also be purchased from those who are trading in such lists, spammers included.[36] Bankrupt businesses also sell their client databases to settle

[27] Ebersöhn supra n 21 764; Shostak *CyberUnion Handbook* 83-4, where the author lists the following ideas on how to support ones effective and safe exploration of the Internet: establishing multiple e-mail accounts; learning to use e-mail filters; learning how to recognise fake e-mail addresses; and verifying attachments by checking with the sender.

[28] Mercado-Kierkegaard (2005) 21/4 *Computer Law & Security Report* 314, where the author lists two types of cookie namely: persistent; and session cookies. "Session cookies are temporary and are erased when the browser exits. As these cookies are discarded after one leaves a site they do not present the same tracking problems as "persistent cookies" which remain on the individual's hard drive until the user erases them or until they expire". See too Idler supra note 8 41- 2.

[29] Hoofnagle et al supra note 10 281-5; and Bowman (2012) 7/3 *Journal of Law and Policy for the Information Society* 725-30 for a discussion on flash cookies or zombie cookies; history sniffing; and device fingerprinting.

[30] Big data when used by vendors may refer to "the technology, which includes tools and processes that an organization requires to handle the amount of data and storage facilities". See Webopedia 'Big data' http://www.webopedia.com/TERM/B/big_data.html (date of use: 4 March 2016).

[31] Motloung (2015) *IMM Journal of Strategic Marketing* 18; and Roos 'Data privacy law' 367-8.

[32] See Webopedia 'Big data' supra n 30.

[33] Motloung supra n 31 18.

[34] Raz U 'How spammers harvest e-mail addresses' http://www.private.org.il/harvest.html (date of use: 10 November 2015).

[35] AtomPark Software 'How to gather email addresses and create mailing lists' http://www.massmailsoftware.com/ezine/past/2003-03-05.htm (date of use: 10 November 2015).

[36] Asscher & Hoogcarspel *Regulating Spam* 69.

debts.[37] Some lists are collected from public web sites which display employees' personal information.[38] This practice is also encouraged by those in the marketing business,[39] hence products or services are offered free of charge provided that users furnish valid e-mail addresses which are then used as spam targets.[40] Various methods are also used to harvest such lists including: "web crawlers";[41] the use of software such as "harvesting bots" or "harvesters". Fingerman notes that harvesting causes two main types of harm:[42]

> first, automated scanning can overburden a server with queries, and secondly, as many Internet users are aware of harvesting techniques and try to avoid them, this has a chilling effect on the use of the web and discussion fora. This leads to users refusing to post their addresses on media platforms for fear that they will be inundated with spam. This reluctance to display contact information has been noted as stifling communication and also harming free speech interests.

Some are of the opinion that harvesting of e-mail addresses is very bad business etiquette and that an honest etiquette is indicative of an honest business.[43] With this in mind, consumers are cautioned about such practices and suggestions on how to reduce the process of their e-mail adressess from being harvested on the Internet are also provided.[44]

[37] Ibid. Also Smith (2004) 16 *SA Merc LJ* 600-01; and Raz 'How spammers harvest e-mail addresses' supra n 34.

[38] Most organisations display their employee's personal information on their web sites. Other lists can be acquired from government departments which require certain information to be made public. See South African Government 'Get Deeds Registry information' (date of use: 10 November 2015).

[39] Bonar A 'Buying e-mail lists cheaper than e-mail list rental?' http://emailexpert.org/buying-email-lists-cheaper-than-email-list-rental/ (date of use: 10 November 2015); also Solomon D 'Harvesting e-mail addresses' http://www.businesstoolchest.com/articles/data/ 20010305130908.shtml (date of use: 10 November 2015).

[40] See Poteet *Canning Spam* 6-8; also Rimmer SW 'Death of spam' http://www.mindworkshop.com/nospam.html (date of use: 10 November 2015).

[41] Id Poteet 14-5. Web crawler is referred to as "a computer program that automatically retrieves web pages for use by search engines". Dictionary.com 'Web crawler' http://dictionary.reference.com/browse/webcrawler (date of use: 10 November 2015). Web crawlers, robots, and spiders are various names given to "the tools used for traversing the web and cataloging the information found". Spiders are used to feed pages to search engines and are so called because they crawl. Webopedia 'Spider' http://www.webopedia.com/TERM/S/spider.html (date of use: 10 November 2015). Market researches are set to use web crawlers to determine and assess trends in a given market.

[42] See Fingerman (2004) 7/8 *Journal of Internet Law* 1-14.

[43] Solomon 'Harvesting e-mail addresses' supra n 39; and Patel A 'How spammers get your number' http://www.citypress.co.za/business/how-spammers-get-your-number/ (date of use: 10 November 2015).

[44] See Surf-in-the-Sprit 'How spammers reap what you sow' http://www.surfinthespirit.com/the-web/harvesting.html (date of use: 10 November 2015); and Raz 'How spammers harvest e-mail

3.2.4 Dictionary attacks

Dictionary attacks – also known as “brute force” or “direct harvesting” attacks – involve spammers sending unsolicited messages to hundreds or thousands of addresses, usually with the same domain name.[45] In this case e-mails are sent to thousands of addresses on a particular domain, the non-existent ones are discarded, while the ones determined to be genuine are compiled into lists and then sold.[46] With this method computers generate every possible combination of letters and numbers on a particular domain, for example, “….@yahoo.com”.[47] These e-mail addresses are generated based on words from a “dictionary” of possible likely words, combined with the domain being attacked.[48] This is done to compile a list of deliverable e-mail addresses for future spam communications.[49] Dictionary attacks are also used as a means of obtaining passwords to gain unauthorised access to computer systems.[50] It has been noted that “dictionary attacks are a major burden to corporate e-mail systems, because these systems usually process nearly all the messages sent to them, even those sent to invalid addresses are

addresses’ supra n 34 where the following methods of harvesting are outlined: “(a) from posts to USENET: spammers regularly scan USENET for e-mail addresses, using programs designed to do that. Some programs just look at article headers containing e-mail address (from, reply-to); (b) mailing lists: spammers regularly attempt to get lists of subscribers from mailing lists (some mailing lists will give these upon request) knowing that the mail addresses are a mixture of valid and a few invalid ones; (c) web pages: this is done using a program which combs through web pages looking for addresses, like e-mail addresses contained in mailto: hypertext markup language (HTML) tags. Some spammer’s even target mail-based pages; (d) web and paper forms: some web sites request various details via forms, for example, guest registers and registration forms. Spammers get these e-mail addresses from those either because the form becomes available on the worldwide web, or because the site sells or gives e-mails to others; (e) web browser: some sites use various tricks to extract a surfer’s e-mail address from the web browser, sometimes without the surfer noticing. Those techniques include, making the browser access one of the pages’ image through anonymous file transfer protocol (FTP) connection to the site, or using JavaScript to make the browser send an e-mail to a chosen e-mail address with that e-mail address configured into the browser; and (f) chat rooms and Internet relay chat (IRC)”.

[45] Washington Times ‘Spammers turn to dictionary attacks’ http://www.washingtontimes.com/business/20040505-092614-5432r.htm (date of use: 10 November 2015) and Poteet supra n 40 22.

[46] Ibid Poteet.

[47] Sullivan ‘Preventing a brute force or dictionary attack: how to keep brutes away from your loot’ http://www.codeproject.com/Articles/17111/Preventing-a-Brute-Force-or-Dictionary-Attack-How (date of use: 10 November 2015); also Quo (2004) 11/1 *Murdoch University Electronic Journal of Law* 1-31; and Walker *Absolute Beginners Guide* 139-40.

[48] Ibid Sullivan.

[49] Quo supra n 47 1-31.

[50] Ibid.

often held before being returned to the sender".[51] While the number of dictionary attacks have in some cases outnumbered legitimate e-mails, some companies have used filters or block all e-mails they think are part of dictionary attacks by recognising the high volume of messages coming from a single source.[52] However, spammers have become sophisticated in that they reduce the number of e-mails sent in each attack, but increase the number of attacks overall.[53]

While dictionary attacks have become more effective in disseminating spam, consumers have gradually learned not to make their addresses public.[54] Users are also less likely than before to sign up for mailing lists unless they know that their addresses will not end up in the hands of spammers.[55] Individuals are also urged to choose e-mail addresses that do not follow established patterns: a mix of letters and numbers, with possible character(s) thrown in, which complicate the processs of 'guessing' an e-mail address.[56]

3.2.5 Spyware

Spyware is software that collects user information through an Internet connection without the user's knowledge, usually for advertising purposes.[57] Spyware is regarded as malware because it installs itself on a computer without the user's knowledge and then monitors the user's computer habits so compromising his or her privacy.[58] Spyware is akin to a 'Trojan horse' in that users unwittingly install the product when they install

[51] Ibid.

[52] Washington Times 'Spammers turn to 'dictionary attacks' supra n 45.

[53] Ibid.

[54] Ibid.

[55] Ibid.

[56] Sullivan 'Preventing a brute force or dictionary attack: how to keep brutes away from your loot' supra n 47; also Quo supra n 47 1-31; and Poteet supra n 40 23.

[57] Webopedia 'Spyware' http://www.webopedia.com/TERM/S/spyware.html (date of use: 10 November 2015); Feinstein *How to do everything* 124-5; Engle (2007-2008) 3/3 *Journal of Law and Policy for the Information Society* 582-3; and Walker supra n 47 123 where the author lists the following as other sneaky spyware techniques: "clicking on a link that downloads spyware from web sites. Spyware can also be embedded in the installation process of a free or pirated piece of software one might have downloaded. Spyware can also get onto one's computer by arriving as an automatic download from web sites one might have visited".

[58] Ibid Walker; also Kapersky Lab 'Malware classifications' http://www.kaspersky.co.za/threats/what-is-malware (date of use: 10 November 2015); Schryen *Anti-spam Measures* 19.

something else.[59] Spyware can take over a user's Internet connection for its own unlawful use such as disseminating spam.[60] It can also take the form of the Internet browser resetting the user's homepage or inserting toolbars into the user's browser that link the user to products or services.[61] Spyware manifests itself on user's computer through sluggish personal computer (PC) performance, weird pop-up-ads, and toolbars that cannot be deleted, and also makes unexpected changes to the users home page settings, and unusual search results.[62] The following have been identified as types of spyware: adware; snoopware; browser hijackers; key loggers; and dialers.[63] Users can protect themselves by using spyware detection and removal utilities,[64] or they can also use anti-spyware software.[65] Once spammers have utilised the above methods in extracting the consumers' e-mail addresses, they are in a position to spoof their spam messages so as to remain undetected.

[59] According to Greek Mythology a "Trojan horse" was "a huge, hollow wooden figure of a horse which was left outside the city of Troy by Greek soldiers pretending to have abandoned their siege of Troy. The Trojans took it into Troy. At night the Greek soldiers who were concealed in the horse opened the gates of Troy to the other Greek soldiers and thus Troy was defeated. In computing terms, Trojan horse means a bug inserted into a program or system designed to be activated after a certain time or certain number of operations". Dictionary.com 'Trojan horse' http://dictionary.reference.com/browse/trojan+horse (date of use: 10 November 2015).

[60] Ibid.

[61] Ibid.

[62] Walker supra n 47 51-2.

[63] Id Walker 48-52. "Adware" is a common name used to describe "software given to the user with advertisements embedded in the application. It is considered a legitimate alternative offered to consumers who do not wish to pay for software". Webopedia "Adware" http://www.webopedia.com/TERM/ A/adware.html (date of use: 10 November 2015). "Snoopware" is "malware that is capable of monitoring one's computer habits on behalf of someone else. This can include parental monitoring software programs designed to track children's computer habits". Techtarget 'Snoopware' http://www.whatis.techtarget.com/definition/snoopware (date of use: 10 November 2015). "Browser hijacking" is "a type of online fraud where scammers use malicious software to take control of a computer's Internet browser and change how and what it displays when the user is surfing the net". See Microsoft 'Fix your hijacked web browser' http://www.microsoft.com/security/pc-security/browser-hijacking.aspx (date of use: 10 November 2015). "Key logger" is "a type of data surveillance software (considered to be either software or spyware) that can record every key stroke one make to log files that are usually encrypted". Webopedia 'Keylogger' http://www.webopedia.com/TERM/K/keylogger.html (date of use: 10 November 2015). 'Dialers' are "programs that initialise a computer's modem and call out silently to a toll line and connect to a web page" (ibid Walker).

[64] Slutsky & Baran (2005) 10 *Georgia Bar Journal* 26.

[65] "Antispyware" is "a type of program designed to prevent and detect unwanted spyware program installations and to remove those programs if installed. Detection may either be rules-based or based on downloaded definition files that identify currently active spyware programs". See WhatIs.com 'Anti-syware software' http://whatis.techtarget.com/definition/anti-spyware-software (date of use: 10 November 2015).

3.2.6 Spoofing (disguising headers)

Spoofing is a technique used by spammers to disguise or to mask their identities.[66] Spoofing is also described as a deliberate attempt to cause a user or resource to perform an incorrect action.[67] Most e-mails are disguised in the header[68] to make it appear as if the e-mail came from somewhere or someone other than the actual source.[69] This is generally done by "exploiting poor authentication measures" in order for spammers to masquerade as someone else.[70]

The following has been characterised as aggravating: addressing schemes that are virtual; domain names that are handed out without verification of the identity of the domain owner;[71] and technical aspects of the Internet which make it easy to forge identifying information that appears in e-mails.[72] The above practices cause problems which affects different stakeholders. Those problems are outlined below.

3.3 Problems caused by spam

3.3.1 No costs to the sender but to the recipients and ISPs

[66] See Poteet supra n 40 104. Spoofing is also "the act of impersonating a machine" (see Downing, Covington & Covington *Dictionary* 453). On the other hand, to spoof is to fool, and in networking the term is used to describe a variety of ways in which hardware and software can be misled. See Margolis *Computer & Internet Dictionary* 523.

[67] See Oxford *Dictionary of Computer Science* 520.

[68] An "e-mail header" is "that part of a message that describes the following: the originator of the message, the addressee or other recipients, and message priority level". See TechTarget 'Header' http://whatis.techtarget.com/definition/header (date of use: 4 March 2017)

[69] See Ebersöhn (2003) *De Rebus* 25-6.

[70] Ibid.

[71] In January 2014 when the new gTLD program of registration for new generic top-level domains was launched, it was noted that spammers were quick to utilise domain names for the distribution of large-scale advertising spam. Shcherbakova T, Vergelis M & Demidova N 'Spam and phishing in the first quarter of 2015' https://securelist.com/analysis/quarterly-spam-reports/69932/spam-and-phishing-in-the-first-quarter-of-2015 (date of use: 10 November 2015).

[72] Rothchild (1999) 74/3 *Indiana Law Journal* 908. Poteet offers the following checklist that individuals should apply before opening a spoofed e-mail: "if an e-mail seems to be out of character for a particular person, first verify its authenticity before over-reacting; if an e-mail's authenticity is in doubt, check the headers to see whether anything appears odd; evaluate how you trust what you read on e-mail, and see whether you need to add a verification step to some of the messages". See Poteet supra n 40 114.

The biggest problem with spam is that the recipients are the ones who have to pay for the spam received.[73] This payment is for Internet access provided by the ISPs as a service cost for using e-mail. The low cost of sending such material is, in turn, the single biggest factor leading to the growth in spam.[74] These costs go beyond the recipients in that each ISPs also has to pay for each and every e-mail message received – the messages which take up a certain amount of the ISPs connectivity and computer bandwidth.[75] This has the effect of slowing down traffic in e-mail transmissions.[76] ISPs end up paying for repairs to servers that crash under the load of the messages being transmitted.[77]

Furthermore, because most spammers spoof (disguise) e-mails, if any e-mail(s) is undelivered it cannot be returned to the sender's e-mail account but is left in the server overloading the system.[78] ISPs are also advised to enlarge their capacity to deal with the volume of spam by paying for sophisticated filters and creating safe lists to block senders.[79] Other costs include the increase in subscription fees for installing filters (in order to block unwanted e-mails), which reduce the intake of spam but does not

[73] Warner (2003) 22 *John Marshall Journal of Computer and Information Law* 144-5. Warner notes the two costs that pass from ISPs to their subscribers as follows: "access costs, which are incurred by the recipients in order to gain access to the Internet. This fee depends on the amount of the data exchanges of both e-mail and non-e-mail. Since e-mail contributes significantly to the extent of data traffic, it also contributes significantly to network access fees. The other one is processing costs which are costs an ISP incurs when it processes e-mail through its computers and into the recipient's inbox, and when it processes e-mail from the sender's inbox through its computers on the way to a regional network. The more e-mail the ISP processes, the greater the costs it incurs".

[74] Simmons & Simmons *E-Commerce Law* 131.

[75] Haase, Grimm & Versfeld *International Commercial Law* 140 where the authors note: "many large ISPs have also suffered major system outages as a result of massive junk e-mail campaigns. If huge ISP can clearly not cope with the flood one should not wonder that small ISPs are unable to cope under the crash of junk e-mail"; and Magee (2003) 19/2 *Santa Clara Computer and High Technology Law Journal* 339.

[76] Ibid Haase, Grimm & Versfeld.

[77] Mayer (2004) 31/1 *Journal of Legislation* 179; also Schryen supra n 58 24-6 where the author discusses the following different types of cost that an ISP incurs: staff costs; infrastructure costs; download costs; legal fees costs; communications and marketing costs; harm through fraud and loss of reputation and opportunity costs et cetera; and York & Chia *E-Commerce* 24.

[78] Simmons & Simmons supra n 74 131.

[79] They also need to use other technologies to reduce the influx of spam, and bear the costs of additional consumer service personnel to handle spam-related subscriber complaints. See Grossman (2004) 19/4 *Berkeley Technology Law Journal* 1542; and Mayer supra n 77 179.

eliminate it.[80] Other costs are felt by legitimate businesses which say e-mail marketing has received a “bad rap” because of spam.[81] These businesses are set to have been “unfairly lumped with spammers in that their discreet and legitimate e-mail marketing and communications are not reaching their audience because of spam-filtering technology”.[82]

3.3.2 Flooding of recipients’ mailboxes

Flooding leads to system crashes and the consumption of massive amounts of memory, storage space, and other resources.[83] The data from undelivered e-mails also requires massive data storage space,[84] and sufficient equipment and personnel to handle the traffic, because the ISP cannot distinguish between legitimate mail and spam e-mails.[85]

3.3.3 Wasting time reading and discarding unwanted messages

Spam has the potential to exceed the volume of legitimate e-mail and overwhelm recipients of such e-mail boxes.[86] A clogged mailbox wastes recipients time in that they must wade through the spam e-mail (reading, deleting, replying, filtering) before they can get to their legitimate e-mails.[87] Spam, therefore, both increases the time spent downloading e-mails resulting in subscription fees being increased as noted in par 3.3.1 above.[88]

[80] Hoffman P ‘Unsolicited bulk e-mail: definitions and problems’ http://www.imc.org/ube-def.html (date of use: 10 November 2015); Haase, Grimm & Versfeld supra n 75 140; also Goldman (2003) 22 *John Marshall Journal of Computer and Information Law* 20-1; and Kamal *Law of Cyber-space* 45.

[81] Chang R ‘Could spam kill off e-mail?’ http://www.pcworld.com/article/113061/could_spam_kill_off_e-mail.html (date of use: 10 November 2015).

[82] Ibid.

[83] Kamal supra n 80 45.

[84] Ibid.

[85] Coalition against Unsolicited Bulk E-mail, Australia (CAUBE.AU) ‘The problem’ http://www.caube.org.au/problem.htm (date of use: 10 November 2015).

[86] See Haase, Grimm & Versfeld supra n 75 141; Hoffman ‘Unsolicited bulk e-mail: definitions and problems’ supra n 80; also Mayer supra n 77 179; and Alongi (2004) 46 *Arizona Law Review* 264.

[87] Systems Publishers ‘South African spam summit announced’ http://www.bizcommunity.com/Article.aspx?c=16&1=196&ai=2347 (date of use: 7 September 2015).

[88] See Coalition against Unsolicited Bulk E-mail, Australia (CAUBE.AU) ‘The Problem’ supra n 85.

3.3.4 Fraudulent practices and objectionable content

Many of the objections to spam relate to its content. For example, some object to receiving commercial messages, particularly those that promote questionable ventures like pyramid schemes and multi-level marketing scams, or contains viruses, et cetera.[89] Others are offended by messages that contain or advertise sexually explicit material, especially those sent to minors (because senders of unsolicited e-mail rarely know the age of persons to whom the messages are sent).[90]

As noted above spammers forge headers and subject lines to create the impression that the messages originate from a source other than the spammer.[91] This is done by offloading return e-mail addresses and complaint handling onto an unsuspecting origin or relay operator by specifying one or more incorrect return addresses in the message itself.[92] By the time the recipient has read through the e-mail message and realised that it is unwanted or objectionable, he or she has been exposed to the content of the message.[93]

3.3.5 Stifling of communication

Spam stifles the efficiency of communication and the free flow of information.[94] It is also set to pose threats to consumer confidence in e-commerce.[95] This, in turn, threatens the mode of communicating as users hesitate to provide their e-mail addresses and thus share ideas with other Internet users.[96] With USENET individuals will either make posts with fake addresses, making replies difficult, or they will avoid posting to USENET at all,

[89] See Magee (2003) 19/2 *Santa Clara Computer and High Technology Law Journal* 339.

[90] Li (2006) 3/11 Webology http://www.webology.ir/2006/v3n1/a23.html (date of use: 7 September 2015).

[91] See Grossman supra n 79 1544; also Hoffman 'Unsolicited bulk e-mail: definitions and problems' supra n 80; and Blainpain & Van Gestel *Use and Monitoring of e-mail* 228.

[92] Ibid Hoffman.

[93] Grossman supra n 79 1544.

[94] Ibid.

[95] Haase, Grimm & Versfeld supra n 75 144.

[96] IT Security 'The 25 most mistakes in email security' http://www.itsecurity.com/features/25-common-email-security-mistakes-022807 (date of use: 10 November 2015).

thus depriving the *fora* of their input.[97] Individuals now avoid putting their e-mail addresses on web pages, because web crawling robots search for e-mail addresses on behalf of spammers as noted above.[98] Once spam exceeds legitimate e-mail, it is said to have the power to reduce or destroy the usefulness and efficacy of e-mail as a modern, fast, and secure communication tool, especially for businesses.[99]

Throughout the years measures have been put in place to eliminate spam, and while these technologies are useful, they have proven to be only part of the solution to this escalating problem. Below follows the discussion on technical measures that have been implemented in order to protect those affected by spam.

3.4 Technical measures for combating spam

3.4.1 Background

Technical measures have been used to limit spam throughout the years. While not all technical measures can be addressed here, a few which are well known and widely used will be covered including: filters; blocking techniques and spam fighters.[100] These are largely used by ISPs in order to protect their clients/users from this scourge.

3.4.2 Types of technical measures in place to combat spam

3.4.2.1 Filters

(a) Background

Filters are the most common anti-spam mechanism used to sort through e-mails before they reach recipients' inboxes. Both recipients and ISPs derive some benefit from the use of filters. Using filters has been noted as being able to reduce time lost from having

[97] Hoffman 'Unsolicited bulk e-mail: definitions and problems' supra n 80.

[98] Ibid.

[99] Haase, Grimm & Versfeld supra n 75 141-2.

[100] See Schreyn supra n 58 59-117 for a discussion of other technical measures in combating spam and a model-driven analysis of the effectiveness of technological anti-spam measures.

to sort through unwanted e-mails before attending to legitimate mail.[101] ISPs, too, can reduce the negative impact of these unwanted e-mails by not relaying them.[102] Poteet puts forward the following options when using filters: “filtering at the client level, running e-mails through an external service, and filtering at server-level if the recipient has control over this level”.[103]

The main reason why filters are not used more often (or not used at all) has been attributed to the fact that the rate of false positives – ie, legitimate e-mail messages that are incorrectly marked as spam – leading to most people being at risk of losing important legitimate e-mails, is more critical than the inconvenience caused by spam messages.[104] Another reason is the fear of losing important e-mails which might have been deleted or relegated to the junk folder by filters.[105] Below is an outline on the different kinds of filters.

(b) Types of filters

Structured text filter

This is the most basic filter which can be built into a number of e-mails, and can enable a recipient to set up rules when matches are made based on the e-mail being scanned.[106] For example, the source code of the message (including header and body) is compared against a list of words, phrases, and text patterns that have been

[101] See Khong (2004) 1 *Erasmus Law and Economic Review* 37.

[102] Ibid.

[103] Poteet further notes the following regarding these filters: “the first type offers the most control and allows users to set up varying rules for what they consider spam, but does nothing to prevent spam from destroying bandwidth; the second deals with spam problem and also places the responsibility for confirguring filters on another party (the external service), however, it has the same level of control as the first. The last one gives more control than the external service, although it does not cut down on bandwidth from the spammer to the server it does, however, it prevents e-mails from being downloaded to the clients” (see Poteet supra n 40 140-2).

[104] Poteet supra n 40 150; and Bindman (2013) 39/4 *William Mitchell Law Review* 1306-09 on the advent of spam filters.

[105] Ibid.

[106] An example of this would be “setting up a name on a subject line like “Viagra” with regular expressions such as [Vv][Ii] and so forth, which would catch the capitalisation of that word, or any other word that one wishes to filter out” (Poteet supra n 40 141).

previously identified as belonging to spam messages.[107] The advantage of this filter is that it can be easily understood and is effective for particular classes of spam, because the reason or command is clear regarding the filter and the message will be picked up as spam.[108] The disadvantage is that this type of filter does not adapt as easily as advanced filters to new forms of spam.[109] Should it happen that the word or phrase has been misspelt it will escape the structured filter.[110]

Heuristic filter

This filter applies a series of rules that add or subtract points from a set spam score.[111] If the spam score exceeds a predetermined number, the e-mail is then classified as spam and appropriate action is taken.[112] This filter has an advantage over structured filters in that "it looks at a variety of indicators such as: the text in the e-mail; colour choices; use of web bugs; e-mail headers; and other characteristics of spam e-mail to determine whether that particular e-mail is spam".[113] The feature can assist in reducing false positives by not flagging e-mails as spam because they contain "bad" or "unsavoury words".[114] The disadvantage is that legitimate e-mail messages can contain many of the indicators that this filter is set to flag, and therefore some effort needs to be made to strike a balance between what indicators to pay attention to and what the threshold should be.[115]

Bayesian filter

[107] See Goodman *Spam Wars* 206-07.

[108] Ibid; Wanli Ma et al *Hoodwinking spam email filters* (Proceedings of the 2007 WSEAS International Conference on Computer engineering and Applications Australia January 17-19 2007) 533-537 http://www.researchgate.net/profile/Dat_Tran11/publication/255665198.Hoodwinking_Spam_EmailFilters/links/54087f860cf2c48563bdc37f.pdf (date of use: 26 November 2015).

[109] Ibid.

[110] Ibid.

[111] Zdziarski *Ending Spam* 29-32.

[112] Ibid.

[113] Ibid; Subramaniam, Jalab & Taqa (2010) 5/12 *International Journal of the Physical Sciences* 1873.

[114] Ibid.

[115] Poteet supra n 40 142.

This type of filter is based on the mathematical probabilities of a given message being spam.[116] Instead of looking for particular phrases or applying rules to determine a spam score, Bayesian filtering compares the style of the e-mail being scanned against a number of lists of e-mails: one that has been previously provided; one containing good e-mails; and one containing spam.[117] This filter makes a statistical analysis of the e-mail and determines the probability of the e-mail being spam.[118] This filter is good at flagging spam and reducing false positives, however, it is difficult to detect whether the filter will flag a particular e-mail as spam or legitimate e-mail.[119]

3.4.2.2 Blocking spam by using blacklists and whitelists

Blocking spam e-mails can be used at domain level where the Internet protocol (IP) address of incoming mail that is offensive is determined and added by an administrator of the network to what is termed a "blacklist".[120] The downside of blacklists is that they require human intervention to block spammers who appear on those lists.[121]

Whitelists on the other hand, are "approved sender lists" which allow users to identify e-mail(s) from approved and legitimate senders.[122] The difficulties associated with whitelists is that while they can assist in reducing spam, they are, however, prone to spoofing or falsification of e-mail source data.[123] In order for these technical measures to be effective, new addresses must constantly be added in order to stop spam from entering mail boxes.[124] Other blocking methods include greylisting which have been credited with being successful in protecting e-mail servers against spam, however, it too

[116] Ibid; Schryen supra n 58 69-71.
[117] Ibid.
[118] Ibid.
[119] Ibid. Subramaniam, Jalab & Taqa supra n 113 1873.
[120] Chigona W; Bheejun A; Spath M; Derakhashani S and Van Belle JP 'Perceptions on spam in a South African context' *Internet and Information Technology in Modern Organisations: Challenges and Answers* 283-291 http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.515.745&rep=rep1&type=pdf (date of use: 20 January 2016); and Zdziarski supra n 111 27-8.
[121] Asscher & Hoogcarspel supra n 36 125; and Subramaniam, Jalab & Taqa supra n 112 1873.
[122] Id Asscher & Hoogcarspel 123; and Schryen supra n 58 64.
[123] Ibid. See also Chigona et al supra n 120 283-291.
[124] Ibid.

has inherent drawbacks.[125] The last part in this chapter focuses on spam fighters and their role in combating spam.

3.4.2.3 Spam fighters

There have been proactive measures put in place to curb spam through organisations whose sole purpose it is to eradicate spam. These spam fighter groups include, but are not limited to, the Coalition against Unsolicited Commercial E-mail and Spamhaus.

(a) The Coalition against Unsolicited Commercial E-mail

The Coalition for against Unsolicited Commercial E-mail[126] was founded in May 1997 by concerned Internet users to advocate for anti-spam laws in the United States of America. It has been instrumental in the discussions around amendments of other anti-spam laws to include e-mail.[127] CAUCE does not assist with spam reports, but directs whomever has complaints to relevant stakeholders.[128] CAUCE also updates individuals on what is taking place regarding spam around the world.[129]

(b) Spamhaus

[125] See Schryen supra n 58 65. Schryen note that "the main problem with greylisting has been the assumption that spammers do not implement the resume feature in order to increase their throughput, thus making it easier for them to circumvent the greylisting".

[126] Hereafter referred to as "CAUCE". CAUCE is a non-profit advocacy group with branches worldwide, that works to reduce the amount of spam via legislation. The Canadian chapter was launched in 1998; followed by Australia in 1998; India later merged into APCAUCE (Asia-Pacific). CAUCE also created an international parent group named CAUCE International (*i*CAUCE). CAUCE North America Inc. was formed in March 2007 from a merger between CAUCE and CAUCE Canada. CAUCE 'About CAUCE' http://www.cauce.org/about.html (date of use: 30 November 2015).

[127] Ibid.

[128] CAUCE 'Spam reporting centers' http://www.cauce.org/spam-reporting-centres.html (date of use: 30 November 2015). CAUCE also collaborates with the following groups: the Messaging Anti-abuse Working Group (MAAWG); the anti-phishing Working Group (APWG); London Action Plan (LAP); and the Internet Corporation for Assigned Names & Numbers (ICANN). CAUCE 'About CAUCE' http://www.cauce.org/about.html (date of use: 30 November 2015).

[129] CAUCE 'Home' http://www.cauce.org (date of use: 30 November 2015).

Spamhaus was founded in 1998 and it is based in Geneva.[130] It is run by 38 investigators, forensic specialists, and network engineers located in ten countries.[131] The Spamhaus project is an international non-profit organisation whose mission is, among others: to track the Internet's spam operation and sources; to provide dependable real time anti-spam protection for Internet networks; to work with law enforcement agencies; to identify and pursue spam and malware gangs worldwide; and to lobby governments for effective anti-spam legislation.[132]

Spamhaus also maintains a number of security intelligence databases and real-time spam-blocking databases responsible for withholding the vast majority of spam and malware sent out on the Internet.[133] In addition to generating real-time reputation data, Spamhaus publishes the Register of Known Spam Operations (ROKSO), a database collating information and evidence on the "100 known professional spammers and spam gangs" worldwide.[134] ROSKO is used by ISPs to avoid signing up known spammers who would abuse their networks, and by law enforcement agencies to help target and mount prosecutions against spam and malware.[135]

3.5 Conclusion

In this chapter, the use of different methods to extract personal information from the Internet by spammers and marketers alike in order to distribute spam was highlighted. It has also emerged clearly that consumers surf the net without considering their privacy and are largely oblivious to the deceptive practices used by spammers and markerts on the Internet. This reveals a lack of education on the consumer's part on how to conduct

[130] Spamhaus 'About Spamhaus' https://www.spamhaus/organization (date of use: 30 November 2015).

[131] Ibid.

[132] Ibid.

[133] These are used by the majority of Internet e-mail service providers, corporations, universities, governments, and military networks. These security intelligence databases include: the Spamhaus Block List (SBL); the Exploits Block List (XBL); the Policy Block List (PBL); and the Domain Block List (DBL). Spamhaus currently protects over 1,9 billion internet user mailboxes (ibid).

[134] Ibid.

[135] Ibid.

themselves, especially in an online environment.[136] Consumers should note some important pointers when surfing the net which include: being on the look-out for and reading the posted privacy statements of individual web sites before divulging their personal information to find out what personal information that web site gathers, and with whom it will be shared; and when filing forms online, they should keep their information private by making sure of its transit across the Internet.[137]

It is also noted in this chapter that while there are technical measures in place to eliminate spam, these have only proven effective to a limited extent, and that while they do not reduce the overall cost associated with spamming, they can substantially avoid the cost of forwarding and storing spam e-mails for their subscribes.[138] The problem, however, persits so proving that the spammer is invariably one step ahead of any measures currently available.

In order to combat spam, research has been undertaken by different stakeholders. In Chapter 4 an examination of the initiatives taken by the international arena in combating spam is undertaken.

[136] Smith (2005) 12/2 *Competition and Consumer Law Journal* 186.

[137] See Idler supra n 8 42. Consumers should also "protect themselves from less reputable sellers online, by looking for sites that clearly disclose the following: the type of business (for example, retailers, online auction); where this business is physically located; how one can contact the business (for example, 800 number); the cost of the products and services; safeguards for protecting payment information; and the availability of warranties or guaranties; sites that can make a significant difference in one's e-mail experience". See O'Neill B (2001) 47 *Consumer Interests* 1; and Poteet supra n 40 10-11.

[138] See Khong (2004) *Erasmus Law and Economic Review* 38.

CHAPTER 4

INTERNATIONAL INITIATIVES TO COMBAT SPAM
ITU AND OECD

4.1 Introduction

In the first three chapters the basis for the study was laid by noting how spam evolved into the scourge it is today. Also the technological measures put in place in order to combat spam were considered. The international arena entered the discourse as far back as the early 2000s lending its voice in this ongoing process. A number of international organisations (some of which were highlighted in the previous chapter), were formed with the sole purpose of creating awareness of this problem, and coming up with solutions. In this chapter focus is on the two organisations which conducts research among others in combating spam, namely: the ITU; and the OECD.

The research undertaken by these organisations has been and remains instrumental in encouraging the transposition of Model Laws to the national level, encouraging mutual agreements in combating spam at a global level, advising regional communities on their initiatives to address the issue of spam, and the question of enforcement.

Here a discussion on initiatives by these two organisations to estabish how this battle has been waged through the years and whether there are solutions in sight for this ever-escalating problem is undertaken. Focus will be on the backgrounds of each organisation, research and initiatives the organisations has undertaken, and the recommendations each has come up with. Surveys, discussion documents, and reports are highlighted to establish whether they offer solutions to the problem.

4.2 International Telecommunications Union (ITU)

4.2.1 Background

The ITU was established in 1865 to facilitate and regulate the interconnection and inter-operability of national telegraph networks.[1] Over the years, its mandate has extended to cover the development of radio-communication and telecommunication, among others.[2] The ITU has also been a specialised agency of the United Nations (UN) since 1947.[3] It has over 190 member states and 700 private-sector members.[4]

The overall objectives of the ITU are to promote the development of telecommunication networks and access to telecommunication services by fostering cooperation between governments and a range of non-governmental actors, which include a variety of role players.[5] The three main sectors[6] of the ITU are: Radio-communications (ITU-R); Telecommunication development (ITU-D); and Telecommunication standards (ITU-T).[7] Focus will be on the ITU-T sector whose mandate it is to research and put forth initiatives in combating spam.

[1] ITU 'Discover ITU's History' http://www.itu.int/en/History/Pages/DiscoveerITUsHistory.aspx (date of use: 30 November 2015).

[2] Ibid.

[3] ITU 'About ITU' http://www.itu.int/en/about/Pages?default.aspx (date of use: 30 November 2015).

[4] ITU '700+ ITU Sector Members & Academia' http://www.itu.int/en/about/Pages/membership.aspx (date of use: 30 November 2015). The ITU is located in Geneva Switzerland and has 11 regional and area offices around the world. It coordinates global networks and services of both governments and the private sector.

[5] These role players include: network operators; service providers; equipment manufacturers; scientific and technical organisations; financial organisations; and development organisations. For the objectives of the ITU see: Article 1 of the Constitution of the ITU 'Collection of the Basic Texts of the International Telecommunication Union Adopted by the Plenipotentiary Conference' (2011 edition, hereafter the 'ITU Constitution') http://www.itu.int/dms_pub/itu-s/oth/02/09/S02090000115201PDFE.PDF (date use: 6 November 2015).

[6] These three sectors are mandated by the Plenipotentiary Conference of the ITU, see art 1 of the Convention of the ITU (2002). For the functions of the Plenipotentiary Conference see art 8 of the ITU Constitution; and ITU 'Sector Members, Associates and Academia' http://www.itu.int/en/membership/Pages/sector-members.aspx (date of use: 30 November 2015).

[7] The Radio-communications (ITU-R) coordinates the vast growing range of radio-communication services, as well as international management of the radio frequency spectrum and satellite orbits. See ITU 'What does ITU do?' http://www.itu.int/en/about/Pages/whatwedo.aspx (date of use: 30 November 2015). The ITU-D has as its core mission to forge international solidarity in the delivery of technical assistance and in the creation and development and improvement of telecommunication/ICT equipment and networks in developing countries. See ITU 'About the ITU-D and the BDT' http://www.itu.int/en/ITU-D/Pages/About.aspx (date of use: 30 November 2015). Each of these sectors activities is directed by international and regional conferences, supported by a bureau under the administration of a director. The bureau directors are in turn advised by advisory groups open to representatives of national telecommunication administrators, authorised organisations, and study groups.

4.2.2 The Telecommunication Standards Sector (ITU-T)

4.2.2.1 Introduction

The ITU-T assembles experts from around the world to develop international standards known as ITU-T recommendations.[8] These recommendations act as defining elements in the global infrastructure of ICT.[9] The framework of the ITU-T sector includes the following groups and/or activities: the World Telecommunication Standardisation Assemblies[10] – an assembly that sets out the overall direction and structure for the ITU-T;[11] the Telecommunication Standardisation Advisory Group[12] which provides ITU-T with flexibility between WTSA by reviewing priorities, programmes, operations, and strategies, among other things;[13] and study groups which represent the standardised work of the ITU-T by technical study groups. Representatives of the ITU-T membership develop recommendations (standards) for various fields of international telecommunication;[14] hold workshops and seminars to promote existing work areas and explore new ones;[15] and Technology Watch, which identifies and surveys emerging technologies and their likely impact on future standardisation for both developed and developing countries.[16]

[8] See ITU 'The framework of ITU-T' http://www.itu.int/en/ITU-T/about/Pages/framework.aspx (date of use: 30 November 2015).

[9] Ibid.

[10] Hereafter referred to as 'WTSA'. The WTSA meets every four years and defines the general policy for the sector, establishes study groups, approves their expected work programmes, and also appoints their chairmen and vice chairmen.

[11] See art 18(2) of the ITU Constitution; and art 13 of the ITU Convention.

[12] Hereafter referred to as 'TSAG'.

[13] The TSAG follows up on the achievements of a particular work program, restructures and establishes ITU-T study groups, and also provides guidelines to the study groups. See art 19 of the ITU Constitution and art 14A of the ITU Convention.

[14] There are a number of study groups conducted in the ITU-T sector, and they work in periods of four years during which they must formulate recommendations. The study groups' work is done primarily in the form of study questions, each addressing technical studies in a particular area of telecommunication standardisation. ITU 'ITU-T study groups (study period 2013-2016)' http://www.itu.int/en/ITU-T/studygroups/2013-2016/Pages/default.aspx (date of use: 30 November 2015); also art 23 of the ITU Constitution; art 14 of the ITU Convention; and ITU 'ITU-T in brief' http://www.itu.int/en/ITU-T/about/Pages/default.aspx (date of use: 30 November 2015).

[15] ITU 'What does ITU do?' supra n 7.

[16] Ibid.

4.2.2.2 Study Group 17

Study Group 17[17] was formed by the merging of study groups 7 and 10 in 2001.[18] SG17 coordinates security-related work across all ITU-T study groups which includes cyber-security, security management, identity management, and countering spam.[19] SG17 has been designated the "Lead Study Group" (LSG) for the telecommunication security sector.[20] The objective of the ITU's study of spam is to help member states and relevant operating agencies to investigate the significance and characteristics of their spam issues.[21]

4.3 Countering and combating spam

4.3.1 Background

[17] Hereafter referred to as 'SG17'.

[18] See ITU 'Short history of study group 17' http://www.itu.int/en/ITU-T/studygroups/2013-2016/17/Pages/history.aspx (date of use: 30 November 2015). Study group 7 was responsible for, among others, data communication, data network and open system communications. See ITU-T 'Study Group 7 area of responsibility (study period 1997-2000)' http://www.itu.int/ITU-T/1997-2000/com07/area-resp-old.html (date of use: 30 November 2015). Study group 10, on the other hand, dealt with languages and general software aspects for telecommunication systems. See ITU 'ITU-T study group 10 (study period 2001-2004)' http://www.itu.int/ITU-T/studygroups/com10/index.html (date of use: 30 November 2015). For a short history of the merger between the two groups see ITU 'Merger of study groups 7 and 10 into new study group 17' http://www.itu.int/ITU-T/studygoups/com07/merger.html (date of use: 30 November 2015).

[19] Other activities in this group include protection of identifiable information, and security of applications and services for the Internet of things (IoT). ITU 'Study group 17 at a glance' http://www.itu.int/en/ITU-T/about/groups/Pages/sg17.aspx (date of use: 30 November 2015); and ITU 'ITU-T work programme' http://www.itu.int/itu-t/workprog/wp_block.aspx?isn=1759 (date of use: 30 November 2015).

[20] Activities of the LSG include: "developing and maintaining security outreach; coordination of security-related work; and identification of needs and assignment and prioritization of work to encourage timely development of telecommunication security recommendations. All study groups are requested to keep SG17 informed of their work plans regarding security so that they can integrate into an overall security work programme". ITU 'ITU-T study group 17 (study period 2005-2008)' http://www.itu.int/ITU-T/2005-2008/com17/tel-security.html (date of use: 30 November 2015).

[21] See ITU-T 'Study groups (study period 2013-2017)' http://www.itu.int/en/ITU-T/studygroups/2013-2016/17/Pages/countering -spam.aspx (date of use: 30 November 2015).

The ITU's initial activities relating to countering spam consisted of a discussion framework for international cooperation.[22] Following the recommendations of the Global Symposium Regulator (GSR) a virtual conference on regulatory cooperation on spam was held on 30 March 2004.[23] In May of the same year, the spam laws and authorities web site was created containing data from more than 40 countries which had adopted anti-spam measures.[24] This web site is updated continuously with information received directly from member states.[25] The web site maintains a webpage dedicated to international cooperation initiatives, providing information on the content and scope of new projects, referring to and linking with the organising or responsible entities, and maintaining an updated list of interesting meetings and conferences on the topic.[26]

The ITU World Summit on the Information Society[27] Thematic Meeting on countering spam followed,[28] where it was noted that: "spam was becoming a major concern taking into account fraudulent activities such as phishing which threatened the confidence in e-mail and the Internet as a whole".[29] The following sessions covering the topics below were held at this meeting: the scope of the problem; technical solutions; consumer education and awareness; spam legislation and enforcement (a cross-border issue); multilateral and bilateral cooperation; and frameworks for international action.[30]

[22] See ITU 'Council 2005: Note by the Secretary-General Report on spam' Document C05/EP/10-E (Geneva 12-22 July 2005) 2 http://www.itu.int/osg/spu/spam/itu-spam-council-report.pdf (date of use: 30 November 2015).

[23] This conference gathered representatives from regulators responsible for countering spam from a number of countries. ITU 'Virtual Conference on Regulatory Cooperation on Spam' http://www.itu.int/ITU-D/treg/Events/semonars/Virtual-events/Spam/index.html (date of use: 30 November 2015).

[24] ITU 'Council 2005: Note by the Secretary-General Report on spam' supra n 22 2.

[25] Ibid.

[26] Ibid.

[27] Hereafter 'WSIS'. See ITU *Legislation and enforcement: a cross-border issue* https://www.itu.int/osg/spu/spam/law.html (date of use: 30 November 2015).

[28] ITU WSIS Thematic Meeting on Countering Spam (Geneva, 7-9 July 2004) http://www.itu.int/osg/spu/spam/presentations/HORTON-OpeningRemarks.pdf (date of use: 30 November 2015).

[29] The chairperson noted in his remarks that "there was a need for improved cooperation in the field, and improving the exchange of best practices between developed and developing countries, creating harmonized legal frameworks and cooperating with other international organizations working in the area". ITU 'WSIS Thematic Meeting on Countering Spam: Chairman's Report' http://www.itu.int/osg/spu/spam/chairman-report.pdf (date of use: 30 November 2015).

[30] Ibid.

In 2005 it was noted that spam had developed into a real threat to the security of e-mails and of the Internet as a whole.[31] Also noted was that spam is a significant and growing business for users, networks, and the Internet as a whole, and that to build confidence and security in the use of ICTs, there is a need to take appropriate action at both national and international levels.[32]

4.3.2 Survey conducted

In realising its objective of countering spam, the ITU conducted a survey among its member states to establish their anti-spam measures or lack thereof.[33] The survey was conducted in 2004 and involved 189 ITU member states.[34] Of the 189 member states who participated, only 58 responses were received.[35] The survey revealed that while a number of countries had implemented anti-spam laws,[36] several countries used alternative laws – such as data protection laws, consumer protection laws, or electronic commerce laws – to address the spam issue.[37] In other countries laws used to enforce spam fell under the jurisdiction of communication regulators and other related bodies.[38] Some countries were in the process of discussing the adoption of specific anti-spam legislation,[39] while several countries had developed no anti-spam legislation at that time.[40]

[31] The meeting was held from 28 June to 1 July 2005. See ITU 'Council 2005: Note by the Secretary-General Report on spam' supra n 22 5.

[32] See para C5 (d) Plan of Action. ITU World Summit on the Information Society 'Plan of Action' Document WSIS-03/GENEVA/DOC/5-E (12 December 2003) http://www.itu.int/net/wsis/docs/geneva/official/poa.html (date of use: 30 November 2015).

[33] See generally Bueti MC *ITU Survey on Anti-spam Legislation Worldwide* ITU WSIS Thematic Meeting on Cybersecurity (Geneva 28 June-01 July 2005) Document: CYB/06 1-62 http://www.itu-int/osg/spu/spam/legislation/Background_Paper_ITU_Bueti_Survey.pdf (date of use: 30 November 2015).

[34] Ibid.

[35] Ibid.

[36] Id 57-8 for survey results. At the time of the survey 26 countries had anti-spam legislation in place. These included: Australia; Austria; Belgium; China; Czech Republic; Cyprus; Denmark; Estonia; Finland; France; Germany; Hungary; Ireland; Italy; Japan; Luthuania; Malta; The Netherlands; Norway; Poland; Portugal; Romania; Spain; Sweden; United Kingdom; and the USA.

[37] Ibid. The 18 countries include: Argentina; Armenia; Brazil; Bulgaria; Canada; Chile; Columbia; Costa Rica; South Korea; Hong Kong; Luxemburg; Malaysia; Mexico; New Zealand; Peru; Russia; and Switzerland.

[38] Id 58.

[39] Ibid. Nine countries were at the time of the survey working on implementing anti-spam laws namely: Argentina; Brazil; Canada; Columbia; Hong Kong; New Zealand; Russia; Singapore; and

4.3.3 Approaches to combating spam by the ITU

The ITU noted that since spam is a serious problem for the Internet it concluded that a single approach to resolving the problem was inadequate and that a coordinated global approach was required.[41] The ITU further observed that spam was a problem impacting on privacy issues, the protection of minors and human dignity, additional costs for businesses, and a loss of productivity. Furthermore, spam was increasingly used in combination with or as a vehicle for viruses.[42] It was further noted that spam generally undermines consumer confidence which is essential for the success of electronic commerce, electronic services, and the development of the information society.[43] The acknowledgment of this problem as one with global implications gave rise to a number of initiatives in the fight against spam.

A coordinated global approach was outlined in Resolutions 51[44] and 52 and included a multi-pronged or comprehensive approach to combating spam. This was reiterated in 2006 when it was noted that this approach should include international cooperation to counter the problems associated with cyber security, including spam.[45] These two

Turkey. Note should be taken here that some of these countries now have anti-spam legislation in place (for example, Canada (2014); Singapore (2008); and New Zealand (2007)).

[40] Ibid. These countries included: Bangladesh; Burkina Fuso; El Salvador; Haiti; Ecuador; Kuwait; Lebanon; Madagascar; Moldova; Morocco; Qatar; Singapore; Syria; and Turkey.

[41] ITU WSIS Thematic meeting on countering spam supra n 28 1.

[42] ITU WSIS Thematic meeting on countering spam 'Multilateral and Bilateral cooperation to combating spam' (2004) 1-12 http://www.itu.int/osg/spu/spam/contributions/Background%20Paper Multilateral%20Bilateral%20Coop.pdf (date of use: 30 November 2015); Sarrocco C *Spam the Information Society: Building Frameworks for International Cooperation* (2004) 11 for an outline on the impact of spam 1-28 http://www.itu.int/osg/spu/spam/contributions/Background%20 Paper_Building%20Frameworks%20for%20Int/%20Cooperation.pdf (date of use: 30 November 2015); Bambauer DE et al *A comparative analysis of spam laws: the quest for a Model Law* (June 2005) 9-10 https://www.itu.int/osg/spu/cybersecurity/docs/Background_Paper_Comparative_Analysis_of_Spam_Laws.pdf (date of use: 30 November 2015).

[43] Ibid.

[44] ITU-T Telecommunication Standardization Sector of ITU *World Telecommunication Standardization Assembly (WTSA)* (Resolution passed in Florianopolis, 5-14 October 2004) 'Resolution 51: Combating Spam' http://www.itu.int/ITU-T/wtsa/resolutions04/Res51E.pdf (date of use: 30 November 2015); ITU-T World Telecommunication Standardization Sector of ITU *World Telecommunication Standardization Assembly (WTSA)* (resolution was passed in Dubai, 20-29 November 2012) 'Resolution 52: Countering Spam' (which has been renamed 'Countering and combating spam' 1-5 http://www.itu.int./dms_pub/ITU-T/opb/res/T-RES-T.52-2012-PDF-E.pdf (date of use: 30 November 2015).

[45] ITU-T World Telecommunication Development Conference WTDC-06 'Mechanisms for enhancing cooperation on cybersecurity, including combatting spam' (Document 116 (Rev.5)-E (12 April

resolutions were later combined to form a consolidated 'Resolution 52' on countering and combating spam.

4.3.4 A comprehensive or multi-pronged approach to combating spam (Resolution 52)

4.3.4.1 Background

The ITU considered that exchanging e-mails and other forms of telecommunication over the Internet had become one of the main means of communication between people around the world.[46] The ITU also noted that with a variety of definitions for spam, it was clear that spam has become a widespread problem resulting in potential loss of revenue for ISPs, telecommunication operators, mobile telecommunication operators, and business users alike.[47] Countering spam by technical means burdens affected entities, including network operators, ISPs, and users who receive spam against their wishes.[48]

Further, spam is often used for criminal, fraudulent, or deceptive activities and is a global problem that requires international cooperation if solutions are to be found.[49] Addressing the issue of spam has become a matter of urgency and that a "multi-pronged" or "comprehensive approach" to combating spam was important. Resolution 52, which outlined the following multi-pronged approach: strong legislation; the development of technical measures; the establishment of industry partnerships to accelerate the studies; education; and international cooperation.[50] All five elements will be discussed in order to review the recommendations and or guidelines mooted.

4.3.4.2 Strong legislation

(a) Introduction

2006)) https://ccdcoe.org/sites/default/files/documents/ITU-060315-CoopInCSpam.pdf (date of use: 30 November 2015).

[46] See Resolution 52 pars (a)-(k) supra n 44.

[47] Ibid.

[48] Ibid.

[49] Ibid.

[50] Resolution 52 (c) (i-v) supra n 44.

First on the list of a multi-pronged approach to combating spam is strong legislation. According to the ITU, "legislation is a fundamental tool in the anti-spam battle and care must be taken in enacting appropriate and efficient legislation in conjunction with appropriate enforcement".[51] And that spam is a "horizontal issue" touching different aspects of telecommunications, trade, privacy and consumer protection.[52] Therefore, the legal framework that must be put in place to combat spam is complex owing, in particular, to the multitude of laws that have been enacted and differing national authorities which deal with the topic.[53]

The first step to strong legislation is to identify and use or create laws to prohibit spam in one's country.[54] For the ITU, there is a need not only to embrace national approaches to spam, but also to be clear on the international component of those anti-spam responses as, realistically, no one is able to stop spam on his or her own.[55] Each set of laws should be seen as part of a web of anti-spam legislation stretching around the globe.[56] The ITU noted that the first anti-spam law was enacted when an average e-mail user received approximately one unsolicited commercial e-mail message per week, and since then the volume of spam has increased.[57] The ITU further noted that while countries have enacted anti-spam laws, those laws have largely been "sentimental laws" and were passed for purposes of having legislation in place.[58] Little effort or design was put into how these laws were to be enforced.[59] Those who had anti-spam legislation in place were seen to have failed to harmonise their legislation so as to provide greater protection for their consumers by ensuring that the laws not only protect

[51] See ITU WSIS Thematic workshop on countering spam 'Discussion Paper Countering Spam: How to Craft an Effective Anti-Spam Law' 1-15 at 4 and 8 http://www.itu.int/osg/spu/spam/contributions/Background%20Paper_How%20to%20craft%20-effective%20anti-spam%20law.pdf (date of use: 30 November 2015).

[52] Ibid.

[53] Sarrocco supra n 42 14.

[54] Ibid.

[55] Ibid.

[56] Ibid.

[57] Bueti supra n 33 8-9.

[58] See ITU WSIS 'Discussion Paper Countering Spam: How to Craft an Effective Anti-Spam Law' supra n 51 4.

[59] Ibid.

users nationally, but that they also do so internationally.[60] Adopting effective legislation was seen as the first and essential step in combating spam. And while legislation may not on its own be sufficient, it was seen as a minimum necessity to cope with spam to define the rights and obligations, and thereby ensure as much legal certainty as possible.[61] In dealing with this issue the ITU noted that while there were anti-spam legislation in place, there were also challenges facing its implementation.

(b) Challenges in implementing legislation to combat spam at national level

The ITU observed that in countries with anti-spam laws, there was a trend towards adopting spam-specific regulation rather than simply applying general-purpose laws to electronic communications.[62] It also noted that spam posed unusual challenges to regulation given its cross-border context and unique financial structures.[63] Legislators were advised to adopt rules aimed specifically at spam and emphasise the need to align existing laws[64] for example, data protection and anti-fraud provisions – with these new rules to ensure that the theories underlying the regulations are coherent.[65] These laws vary considerably in their approach to tackling the issue of spam. This includes the way in which countries define the term spam and the mechanisms they use to regulate it.[66] These countries also set requirements subject to which unsolicited communications can be sent. These requirements are discussed in greater detail below.

(c) Requirements for strong anti-spam legislation

Definition of spam

[60] Ibid.
[61] ITU WSIS 'Multilateral and bilateral cooperation to combat spam' supra n 42 3.
[62] Bueti supra n 33 9.
[63] Ibid.
[64] Bambauer et al supra n 42 10-11.
[65] Ibid.
[66] Sarrocco supra n 42 14. For e-mail to be legitimate, many anti-spam instruments required as a general rule that the unsolicited mail must be commercial in nature.

The ITU noted that there is no agreed definition of spam generally accepted by stakeholders embodied in anti-spam laws.[67] Therefore, the initial decision for legislators when assessing spam, is whether to differentiate between messages on the basis of their content or of their purpose.[68] A further characteristic is that spam is sent in bulk – whereby the sender distributes a large number of essentially identical messages and recipients are chosen indiscriminately.[69] Many spam laws focus on messages with a commercial content which presupposes the advertising of products and services addressed to recipients.[70]

While there is disagreement and confusion as to the precise definition, it was noted that there is fairly widespread agreement that spam exhibits certain general characteristics. First, spam generally takes the form of an electronic message – in most cases restricted to e-mail but there are other methods of delivering spam including: SMS; Voiceover Internet Protocol (VoIP); and mobile phone multimedia messaging services.[71] Secondly, spam is unsolicited in that no consent is given for the receipt of the messages.[72]

Mechanisms for regulating spam

The ITU advised that in order to regulate spam, legislators should, in the initial phase, determine whether unsolicited messages are permitted or forbidden.[73] To that end, anti-spam legislation should either adopt the "opt-out mechanism", or the "opt-in mechanism".[74] These mechanisms, while common, vary from country to country. Opt-in regimes focus on the means of obtaining, recording, and revoking consent, while the

[67] Ibid.

[68] Bambauer et al supra n 42 16.

[69] Ibid.

[70] Ibid. The ITU noted for instance, that Japan's spam laws only apply to organizations that make profit or individuals engaged in business, while Australian spam laws expressly do not apply if they affect the constitutional right of political parties.

[71] Bueti supra n 33 7. Bueti noted that "in some countries applications relates specifically only to e-mail and that communications by other applications are covered by other regulators. In such cases regulators also need to decide whether the laws will cover other applications such as dealing with spam only in the context of e-mail or SMS texts et cetera".

[72] Ibid

[73] ITU WSIS 'Discussion paper countering spam: how to craft an effective anti-spam law' supra n 51 3.

[74] Ibid.

opt-out regime concentrates on how recipients can indicate that they do not wish to receive messages.[75]

(i) Opt-in mechanism

This mechanism requires prior consent from the recipient before any marketing correspondence can be sent.[76] The opt-in mechanism discourages marketers from sending spam to consumers unless they have clearly asked to receive those messages.[77] The ITU noted that "those who adopt this approach are making a statement that marketers should not send messages to recipients unless those recipients have expressly asked to receive such communications".[78] Under the opt-in approach affirmative requests for messages may be delivered directly by a recipient in the form of an actual request, or consent can be constructively construed if the sender has an existing business relationship with the recipient.[79] The ITU noted in some jurisdictions that have adopted this approach, also create an exception for business entities with which recipients have a pre-existing business relationship.[80] In that case, member countries could choose between the opt-in and opt-out approaches, provided that they respect the legitimate interests of subscribers with regard to unsolicited communications.[81]

The ITU pointed out that the critics of the opt-in mechanism contend that it unreasonably burdens legitimate business.[82] Direct marketers have in this case cited statistics to show that some e-mail users wish to receive unsolicited offers via e-mail,

[75] Bambauer et al supra n 42 17.

[76] Sarrocco supra n 42 15.

[77] Ibid.

[78] ITU WSIS 'Discussion paper countering spam: how to craft an effective anti-spam law' supra n 51 5.

[79] Ibid. For example if one buys a product under this approach, the merchant may send an offer(s) in the future until one asks that merchant to stop.

[80] This exception is applicable only to advertisements of similar products and services and the address must be used by the same person who legally collected the original data. Sarrocco supra n 42 15.

[81] Ibid.

[82] ITU WSIS 'Discussion paper countering spam: how to craft an effective anti-spam law' supra n 51 5-6

and that closing that channel entirely would be overly restrictive and burdensome.[83] The ITU also noted that approximately one-third of anti-spam laws are considered to have adopted the opt-in mechanism.[84] It also observed that although these laws have proliferated over the years, prosecutions under them remain virtually non-existent.[85] The ITU further noted that any anti-spam regime with an opt-in system at its core, is almost certain to offer a more aggressive anti-spam regime than the opt-out system.[86]

(ii) Opt-out mechanism

As regards the opt-out mehanism, the ITU noted that this regime considers direct marketing, and therefore unsolicited commercial communication, a legitimate activity unless certain conditions are not respected.[87] The opt-out approach advocates that a sender may send a message to a recipient even if there is no existing business relationship. It is important to note that the recipients must have not specifically elected to receive such messages.[88] Laws that advocate for this mechanism, typically require the sender to honour the requests of recipients to be removed from its mailing list.[89]

Critics of the opt-out mechanism note that this mechanism legalises spam because it does not expressly provide that the sending of unsolicited e-mail messages is illegal.[90] Instead, this mechanism provides a framework under which such messages may be sent as a result exacerbating the problem.[91] It is noted that most users already have strong preconceptions regarding spam, and they have been widely advised not to open or reply to any spam messages to avoid confirming that their e-mail addresses are

[83] Ibid.

[84] Ibid. Countries that have adopted the opt-in mechanism include: Australia; Singapore; and New Zealand. The Australian position in combating spam is discussed in Chapter 7 below.

[85] Ibid.

[86] Bambauer et al supra n 42 17.

[87] Sarocco supra n 42 15.

[88] ITU WSIS 'Discussion paper countering spam: how to craft an effective anti-spam law' supra n 51 5; and Sarrocco supra n 42 15.

[89] Ibid. In this instance, unsolicited messages may be sent but senders should refrain from sending such upon a request from recipients.

[90] ITU WSIS 'Discussion paper countering spam: how to craft an effective anti-spam law' supra n 51 5

[91] Ibid.

active.[92] The ITU observed that approximately two-thirds of world's anti-spam laws can be regarded as expressions of the opt-out mechanism.[93] It noted further that two of the most effective anti-spam laws originated in two states in the USA which have adopted the opt-out mechanism as their default mechanism.[94] The same was later adopted by the federal law in 2003. Even the OECD noted that while these laws appeared to have been weak on paper, they managed to address the practical problems prosecutors face when enforcing laws against spammers.[95] Regarding these two mechanisms (opt-in and opt-out) the ITU noted that the lesson to be learned is "that the strength of the sentiment in a specific law bears little correlation to the successful enforcement of that law".[96]

Note should be taken here that the first two requirements – the definition and the mechanisms – are found in most anti-spam laws currently in force. However, in most jurisdictions the requirements that follow do not necessarily apply either in whole or in part. In the discussion below I continue by outlining additional requirements for anti-spam laws.

Fraudulent or misleading header information

(i) Background

The ITU defines a subject line as part of the message body which is generally displayed by a user's e-mail application system along with the sender's name and address.[97] It is common cause that spam messages often contain false subject lines designed to lure

[92] Sarocco supra n 42 16.

[93] Id 17. The ITU noted that countries such as the USA; South Korea; and Columbia have adopted the opt-out mechanism.

[94] ITU WSIS 'Discussion paper countering spam: how to craft an effective anti-spam law' supra n 51 5-6. The two states are: Virginia and Washington. The provisions of those states and the USA's Federal Law are discussed at length in Chapter 6 where the anti-spam laws of the USA are highlighted.

[95] Ibid.

[96] ITU WSIS 'Discussion paper countering spam: how to craft an effective anti-spam law' supra n 51 6.

[97] Id 20.

users into opening and viewing the messages.[98] The ITU noted that a common concern regarding subject-line requirements is "the burden they place on legitimate law-compliant advertisers while having no effect on non-compliant senders".[99]

(ii) Disguising sender identity

According to the ITU, most anti-spam laws prohibit messages that contain fraudulent, deceptive or misleading information – for example, an incorrect representation of the sender's identity, e-mail address, or affiliation.[100] This further includes an incorrect opt-out address for users to decline further communication,[101] or where the purpose of the message and its routing path (including message headers)[102] are incorrect.[103] It is noted that these provisions are important to the aim and application of spam legislation, because if senders were to be allowed to defraud recipients, consumers would be less willing to engage in electronic commerce.[104]

Messages with fraudulent sender addresses are set to harm innocent third parties who may suffer significant reputational damage, and who may incur significant costs when consumer complaints are erroneously sent to them.[105] The ITU noted that the falsification of the sender's identity in the header message makes law enforcement more difficult and further adds to user costs – especially senders whose addresses are frequently disguised.[106]

(iii) Use of labels

[98] Ibid.

[99] Ibid. Bambauer et al supra n 42 20.

[100] Bambauer et al supra n 42 16.

[101] Ibid.

[102] A "header" is part of the message that describes the originator; the addressee; other recipients; priority of a message; subject of the message et cetera. WhatIs.com 'Definition header' http://whatis.techtarget.com/def/header (date of use: 30 November 2015).

[103] Ibid.

[104] Ibid.

[105] Ibid.

[106] Id 14.

The ITU noted that the label requirement is common but varies from one legal system to another. Spam messages are required to have a subject line containing the following characters “ADV” to enable recipients to set filters to delete or quarantine all messages with “ADV” in the subject line.[107] This approach seeks to enable users to identify spam messages easily by requiring that the subject line contain a distinctive identifier such as a series of characters.[108] This condition is often imposed for messages having sexually explicit content to warn the recipient of the content and, in particular, to avoid it reaching children who are often the unintended recipients of this form of spam.[109]

Labels for commercial messages have also been imposed in that the use of tags in the subject line of an e-mail is visible, and so allows users to identify commercial messages more easily.[110] This is set to be in order to allow users to make use of filters which redirect those e-mails to a specific folder, or to avoid children receiving e-mail messages with pornographic content.[111] The ITU noted that labeling requirements may increase the volume of non-compliant messages as marginal senders may choose openly to disregard the law rather than increase the likelihood that their messages will be deleted by filters.[112]

The ITU reckons that additional quantitative research would be useful in this area because the merits of such requirements depend on an empirical assessment of how frequently users filter messages based on subject lines.[113] Furthermore, how often recipients respond to messages with misleading subjects, and what level of blocking of complaint messages is acceptable in achieving a given reduction in non-complaint messages, would also be helpful.[114] Sarocco notes that the problem with this requirement is that the labeling rule is difficult to enforce in respect of anonymous

[107] Ibid.
[108] Ibid.
[109] Sarocco supra n 42 15.
[110] Ibid. The Republic of Korea was noted as one of those countries that require such listing.
[111] Bambauer et al supra n 42 21. Countries such as Spain; South Korea and the USA were noted as requiring labelling messages with “Advertising” and “ADV” respectively.
[112] Ibid.
[113] Ibid.
[114] Ibid.

spammers, and that this might be ascribed to labels being decided at national level and so varying from country to country.[115]

Aggravating violations

In order for an e-mail to be legitimate, many anti-spam laws require that a procedure governing address gathering which respects the right to privacy in the processing of personal data in the electronic communication sector be followed.[116] According to the ITU, aggravated violations include the use of address harvesting and dictionary attacks which are outlined below.

(i) Address harvesting

The ITU noted that harvesting inhibits the use of e-mail addresses on the Internet as a contact method, and subjects users who use their addresses in an unrelated context to a barrage of spam.[117] It was also noted that the use of address harvesting tools is prohibited, and gathering addresses in this fashion, whether manually or using software tools, is unlawful in certain jurisdictions.[118]

(ii) Dictionary attacks

The ITU noted that software programs can automate address gathering and use algorithms to create more realistic addresses than random generation would produce.[119] In this case, spammers attempt to send messages to each of these addresses even though many, if not most, do not correspond to actual users.[120] This has two detrimental effects: “first, the large number of inaccurate addresses place a considerable load on ISP servers with no corresponding benefit; and secondly, it results in messages that are

[115] Sarocco supra n 42 15.
[116] Ibid.
[117] Bambauer et al supra n 42 18.
[118] Ibid. The USA and Australia are among the countries that have this as a provision in their anti-spam laws. These are discussed in Chapters 6 and 7 below.
[119] Id 18.
[120] Ibid.

unsuccessfully transmitted to be poorly targeted since the recipient is selected at random”.[121] The transmission of messages to addresses created in this way is often prohibited.[122]

(iii) Software tools for address harvesting and dictionary attacks

The ITU noted that spam laws prohibiting address harvesting and dictionary attacks also outlaw the creation and use of software that performs these functions.[123] The aim of these prohibitions is to make the dissemination of spam more difficult by reducing the number of automated tools that produce addresses.[124] Secondary liability was also noted as important because it is faster and easier for a spammer to purchase lists of e-mail addresses than to collect them (either manually or using software tools).[125] In this light, banning the use and sale of lists generated by the use of authomated tools helps prevent spammers from avoiding liability.[126]

(iv) Publicly disclosed addresses

Senders might seek to communicate with the general public (for example, a political candidate who posts an address on his or her campaign site, or any other public figure who posts an address that might be of importance to the public).[127] Existing regimes treat publicly disclosed addresses differently when it comes to whether their collection

[121] Ibid.

[122] Ibid. Countries such as South Korea prohibit using any program that creates recipient contact information such as e-mail addresses or telephone numbers by combining letters, marks and numbers.

[123] Id 19. Japan prohibits programs that generate random, fictitious addresses, while South Korea bans using, distributing, or selling addresses gathered using such software tools if the user knows that the collection of the addresses violated the prohibition on aggregating them from web pages against the terms of service on those pages.

[124] Ibid.

[125] Ibid.

[126] Ibid.

[127] South Korea prohibits gathering and using e-mail addresses posted on web sites only if the sites post terms prohibiting such collection and use. Argentina, on the other hand, would seem to permit collection of e-mail addresses which qualify as personal data under its Personal Data Protection Act if those addresses are posted on publicly available web sites (Bambauer et al supra n 42 19).

and use should be prohibited.[128] The assumption here is that those recipients have implicitly consented to receive unsolicited messages.[129]

(v) Requirements for the destruction or removal of addresses

Once recipients have indicated that they no longer wish to receive communications from a particular sender, the sender may be legally obliged to remove information such as e-mail addresses from its records.[130] Such a mandate finds greater application in an opt-in regime where only recipients who have consented to receiving messages may be lawfully contacted, than in an opt-out regime where senders might need to retain the e-mail addresses of users who unsubscribe in order to track to whom messages should be sent.[131]

Unsubscribe requirement

The ITU noted that anti-spam legislation often contains a requirement that the sender of a message include a means by which recipients can indicate that they no longer wish to receive messages from that sender, or messages dealing with the specific topic, along with an instruction that the sender adhere to the recipient's wishes.[132] Although the unsubscribe requirements are important in an opt-out regime, they are also useful in an opt-in system as they allow a recipient to change his or her mind and revoking permission to communicate with the sender in future.[133]

The ITU noted that legislation may, however, prescribe one or more ways in which recipients wishing to unsubscribe are able to communicate with the sender – for example, through a working e-mail address, or a phone number. Some anti-spam laws

[128] Ibid.

[129] Ibid.

[130] Ibid.

[131] Ibid.

[132] The following countries were noted as compelling senders of unsolicited communication to honour such a facility: USA; Australia; and Argentina. Argentina is noted as permitting recipients to demand that a sender remove their addresses from the sender's database. Ibid.

[133] Ibid.

also dictate characteristics for an unsubscribe process which include requiring the sender's unsubscribe mechanism to remain functional for at least 30 days after a message has been sent, and prohibiting senders from imposing costs on recipients who opt-out.[134] Laws may also specify which languages the unsubscribe mechanism must use – for example, the country's official language(s).[135]

The ITU notes that for the unsubscribe requirement to be effective senders must:[136] "honour the request (some senders may ignore these requests or may seek to evade them by closing the e-mail addresses used to gather such requests rapidly and shifting to a new one); and recipients must have sufficient confidence in the efficacy of the unsubscribe methods in order to use them". Failing this, if the opt-out addresses are non-functional recipients cannot choose what advertising to receive and what to reject.[137]

Users are also cautioned against using the unsubscribe mechanism as there is no guarantee that senders will comply with their requests, and that in attempting to unsubscribe they will in fact confirm their existence.[138]

Penalties

The ITU noted that many legal regimes adopted multiple types of penalties for violating spam laws.[139] These penalties falls within the following three categories: administrative penalties imposed by an enforcement entity for less serious offences; civil damages (actual or statutory) imposed by an adjudicating court; or criminal penalties for more serious and harmful offences (imposed by a court in criminal prosecutions).[140] Other penalties often encountered include provisions specifying increased penalties for repeat violators, and provisions allowing entities harmed by spam to seek injunctive relief to

[134] Id 20. Countries that have that as a provision include USA; South Korea; and Australia.

[135] Ibid.

[136] Ibid.

[137] Id 16.

[138] Id 20.

[139] Ibid.

[140] Id 26.

mitigate or prevent future harm.[141] The ITU noted that the level and type of penalty imposed in spam laws should reflect both subjective judgment and criteria as to the relative gravity of the harm in question, and also how to enforce the relevant law effectively.[142] It is also noted that how penalties are structured may also present challenges for enforcement in that spam laws may provide for statutory damages for violations because of the difficulty of quantifying the harm caused by spam message(s).[143]

The problem of proof is also a form of deterrence enforcement by allowing violators to evade penalties when evidence of quantifiable harm is lacking.[144] As a result, by increasing the costs and uncertainty of recovery for enforcers, statutory damages encourage enforcement and increase deterrence.[145] The ITU noted that administrative penalties are viewed as useful in that administrative agencies often use less formal and more rapid adjudication measures than a court system.[146] This reduces the cost of enforcement and can help improve compliance.[147] In addition, an agency whose scope is limited to data or consumer protection may be more focused and better equipped to deal with a problem like spam than an entity with broad law-enforcement responsibilities.[148]

Enforcement

The ITU advised that enforcement of anti-spam provisions should be addressed at both national and international levels.[149] Practical issues relating to enforcement – eg, jurisdictional questions – are the most significant barriers to developing effective legal

[141] Ibid. Countries such as the USA and Australia have put these penalties in place.
[142] Ibid. Criminal penalties may be used in these cases to punish particularly grave harm such as that involving victims who are minors or to create deterrence where identifying the violator is difficult or rare.
[143] Ibid.
[144] Ibid.
[145] Ibid.
[146] Ibid.
[147] Ibid.
[148] Ibid.
[149] Sarocco supra n 42 17.

responses to spam.[150] E-mail is generally unaffected by national boundaries because of the borderless nature of the Internet, and many e-mail addresses provide no indication of their physical location while e-mail addresses which include a geographic identifier can be used from anywhere in the world.[151] In addition to the above, the ITU noted that enforcement of the provisions regarding unsolicited communications is not performed by the same authority in all countries.[152] For example, it was noted that in most countries in which spam is treated as a breach of privacy, a Data Protection Authority (DPA) decides on the application of the law and on enforcement of the rules.[153] In other instances, a National Regulatory Authority (NRA)[154] for telecommunications may be involved; while in yet other cases, the Consumer Protection Authority fulfills this role.[155]

The ITU observes that while most countries regulate spam, there continue to be only a limited number of spam cases that end up before the courts.[156] This is perhaps due to the fact that spammers are using increasingly sophisticated techniques to hide their identities and the origin of their e-mails, making prosecution a "drawn-out process" which is both time consuming and expensive as the laws regulating spam are territorial while spam is international or borderless.[157] The difficulty of identifying spammers and enforcing the law against those identified, adds to why spamming is so easy and is considered "a low-risk and profitable business".[158] Further, because spammers do not have to bear high operational costs, and given the barriers to law enforcement and anonymity, the threat of punishment is considered an ineffective way of ensuring compliance with anti-spam laws.[159]

[150] Ibid.

[151] Ibid.

[152] Ibid.

[153] Ibid. European Union countries such as Italy and France and beyond the EU Argentina and New Zealand make use of the DPA.

[154] Ibid.

[155] Ibid. The Federal Trade Commission in the USA utilizes the Consumer Protection Agency to enforce spam laws.

[156] ITU WSIS 'Discussion paper countering spam: how to craft an effective anti-spam law' supra n 51 6.

[157] Ibid.

[158] Sarrocco supra n 42 17.

[159] Ibid.

As indicated by the ITU, prosecutors face a number of costs when bringing legal action against spammers.[160] Understanding what those costs are and how to minimise them, is crucial when crafting effective anti-spam legislation.[161] The costs faced by prosecutors in tracking down and identifying spammers are substantial as spammers use multiple techniques to hide their identities.[162] Identification costs would be relatively minor if only a few cases had to be filed.[163] However, cases against hundreds of spammers will probably be required before any real benefit or deterrence can be achieved.[164] These costs can soon become prohibitive for an individual litigant.[165] In addition to the cost involved in tracking down spammers, victims also face the costs of litigation once the target has been identified.[166] Some suggestions have been made to assist drafters of anti-spam laws when they consider enforcement.[167]

In conclusion, the ITU proposes that experts consider the importance of developing effective enforcement measures which empower enforcement agencies to act against the proliferation of spam.[168] These measures should also promote cooperation between the different jurisdictions from which an e-mail user is likely to receive spam.[169] At a national level, the ITU recommends the following initiatives: attention to spam prevention and the dissemination of information through working group hearings involving the principal actors; the creation of education modules; the maintenance of

[160] ITU WSIS 'Discussion paper countering spam: how to craft an effective anti-spam law' supra n 51 6.
[161] Ibid.
[162] Ibid.
[163] Ibid.
[164] Ibid.
[165] Id 7.
[166] Ibid.
[167] These suggestions include: "allocating primary responsibility for enforcing spam law to a single entity within each state that is suitably funded and staff to pursue violations aggressively; establishing explicit coordination, including coordination mechanisms, among entities with responsibility for enforcement (including, private actors such as ISPs); creating a graduated system of penalties, from administrative fines for minor offenses to criminal penalties for major or repeated violations; creating secondary liability for entities that advertise products or services via spam to deter, to encourage advertisers to select reputable communications firms, and set up incentives for advertisers to monitor the communications on their behalf; and establish further Memorandum of Understanding between enforcement officials in multiple regions to facilitate enforcement cooperation." See Bambauer et al supra n 42 35; also ITU WSIS 'Discussion paper countering spam: how to craft an effective anti-spam law' supra n 51 9.
[168] Ibid Bambauer.
[169] Sarocco supra n 42 16.

regular contact with law enforcement officials; and finally, the identification of the fight against spam as a government priority.[170]

(d) Harmonisation of laws

According to the ITU, spam laws, whether harmonised or not, are at best only part of the solution to the problem and must be developed in concert with technical, market, and norm-based tools if the scourge of spam is to be substantially reduced.[171] Although it is crucial to the success of spam legislation that harmonisation of laws through a “Model Law” approach provide consistent responsibilities and penalties, the burden of enforcing these dictates falls to each legal system involved.[172]

The ITU noted that existing regulatory provisions within the states’ legal systems and spam legislation must be aligned.which is to be achieved: first, by legislators who must decide whether to rely on broader, more general-purpose laws; and second, if the “general purpose laws” route is followed, the specific elements in the spam laws must be reconciled with the relevant provisions of the general purpose laws.[173] Regarding the first aspect, the ITU noted that there is a clear trend among individual states to move towards regulations aimed specifically at addressing spam.[174] A number of states do not have rules focused solely on spam and rely instead on data protection laws, common-law suits, consumer- protection statutes, and self-regulation by service providers.[175] It is further noted that creating regulations specifically targeting spam can help focus enforcement efforts, strengthen anti-spam norms, and close loopholes or uncertainties in existing laws that also apply to spam.[176]

[170] ITU WSIS Thematic Meeting on Countering Spam ‘Legislation and Enforcement’ (2004) 1-15 at 3-4 http://www.itu.int/osg/spu/spam/contributions/Background%20Paper_Legislation%20and%20Enforcement (date of use: 30 November 2015).

[171] Bambauer et al supra n 42 21-22.

[172] Id 35.

[173] Id 21.

[174] Ibid.

[175] Ibid.

[176] Ibid.

The ITU also observed, that spam tends to fall under different rubrics including computer misuse and false advertising, to data protection and criminal fraud.[177] Individual states that introduce spam-specific legislation must consider, and ideally specify, how these different pieces of legislation must interact.[178] The ITU, therefore, suggests that for an anti-spam law to serve as a successful deterrent to spammers, its level of effectivity must be increased.[179] By this is meant that, "the next generation of spam laws must be "action laws" and should achieve the following goals:[180] increase the benefit of successful prosecution; reduce the cost of identifying spammers; reduce the cost of prosecution; increase the probability of success at trial; and reduce any external costs to society arising from investigating and bringing a spammer to trial". This is hoped will give prosecutors the tools and resources they need to effectively track down and prosecute spammers.[181] Every legislature will, however, need to adapt its own regulations to emphasise its law enforcer's strength and overcome specific weaknesses within its system.[182]

In conclusion, for nations to succeed in regulating the scourge of spam, they will first have to put laws in place which meet the requirements set out above. Below, a discussion of the remaining four multi-pronged elements are considered, starting with the development of technical tools and best practies.

4.3.4.3 Development of technical tools and best practices

According to the ITU, industry research bodies – and the Internet community in particular – need to continue with the development of technical anti-spam solutions.[183] This work needs to be conducted on the international level.[184] Technical solutions have

[177] Ibid.

[178] Ibid.

[179] ITU WSIS 'Discussion paper countering spam: how to craft an effective anti-spam law' supra n 51 7-8.

[180] Ibid.

[181] Ibid.

[182] Ibid.

[183] Also see Chapter 3 para 3.4.2 above.

[184] ITU WSIS 'Multilateral and bilateral cooperation to combat spam' supra note 42 1-12; also ITU-T Series X Data Networks, Open System Communications and Security (Telecommunication

been noted as representing the user's first line of defence against spam.[185] These anti-spam technologies are in a state of continuous flux due to continual adaptation by spammers attempting to circumvent them.[186] It has been noted that in order to curb spam three different stages in the e-mail system need to be considered and that attention be paid to where technical solutions could be implemented: (a) at source[187] where the e-mail is sent out; (b) at destination[188] where the e-mail is received; and (c) at the end-user point.[189] Most, if not all, anti-spam legislation makes no provision for technical measures to combat spam.[190] These technical solutions are left to other stakeholders – for example, ISPs – using filters to protect recipients from receiving unsolicited mail.[191] The ITU noted that spam-filtering software remains the most popular tool in combating spam and that several different methods should be combined to

security) 'Technologies involved in countering e-mail spam' (Recommendation ITU-T X.1240 (04/2008)) 1-19 http://www.itu.int/ITU-T/recommendations/rec.aspx?rec=9334 (date of use: 30 November 2015). The document outlines the following anti-spam technologies: existence of sender's domain and eliciting a response; blacklists and whitelists; greylisting; and filtering to mention but a few (5-12); also ITU-T Series X: Data Networks, Open System Communications and Security (Cyberspace security countering spam) 'Framework for countering spam in IP based multimedia applications' (Recommendation ITU-T X.1245 (12/2010) 1-23 http://www.itu.rec/T-REC-X.1245-201012-I/en (date of use: 30 November 2015); and ITU-T Series X: Data Networks, Open System Communications and Security 'Supplement on a practical reference model for countering e-mail spam using botnet information' (Series X.1243) 3-6 http://www.itu.int/ITU-T/recommendations/rec.aspx?rec=11755 (date of use: 30 November 2015). This document defines a "botnet" as "a collection of Internet-connected computers whose security defences have been breached and are controlled by an unknown party. Each compromised "bot" is created when a computer is penetrated by software from a malware distribution source, which makes the controller of a botnet able to direct the activities of these compromised computers through communication channels forms by standard based network protocols" (at 1).

[185] ITU-T Series X: Data Networks, Open System Communications and Security (Telecommunication Security) 'Technical framework for countering email spam' (Recommendation ITU-T X.1241 (04/2008)) 1-11 http://www.itu.int/ITU-T/recommendations/rec.aspx?rec=9335 (date of use: 30 November 2015).

[186] Ibid.

[187] For discussion of implementation at the source: see ITU WSIS Thematic Meeting on Countering Spam 'Curbing spam via technical measures: An overview' 1-18 at 3-6 http://www.itu.int/osg/spu/spam/contributions/Background%20Paper_curbing%20Spam%20Via%20Technical%20Measures.pdf (date of use: 30 November 2015); also ITU-T Series X: Data Networks, Open Systems Communications and Security (Telecommunications security) 'Technical strategies for countering spam' (Recommendation ITU-T X.1231 (04/2008) 1-11 http://www.itu.int/ITU-T/recommendations/rec.aspx?rec=9333 (date of use: 30 November 2015) for a general discussion on the following strategies: equipment; network; service; filtering; and feedback strategies.

[188] Id ITU WSIS 'Curbing spam via technical measures: An overview' 7-9.

[189] Id 9-13; also Sarocco supra n 42 12.

[190] ITU WSIS 'Discussion paper countering spam: how to craft an effective anti-spam law' supra n 51 1-16.

[191] Ibid.

provide the best service to users.[192] Filters used at ISP level or directly at the user level can block a high percentage of spam. A natural consequence of this, however, is the possibilty of blocking legitimate mail and so reducing the reliability of electronic communications.[193] The ITU further noted that these filters are soon outpaced by spammers who become increasingly sophisticated in their attempts to evade filtering techniques.[194] And that the constant need to update filters represents a significant additional cost for users and providers.[195]

The ITU noted that collaboration on anti-spam technologies is required across sectors of industry, for example, the Internet and e-mail service providers, network operators (carriers), and software developers.[196] Also included are governments, the technical community, industry organisations, which have a valuable function to fulfil in order to stop this persistent nuisance which has far reaching consequences.[197] The ITU also noted that some technical measures if incorrectly applied may cause more harm than good, and may on their own create little incentive for spammers to curtail or stop their behaviour.[198] Instead, they allow spammers to claim that their activities are harmless or that they are providing a valuable service to the community on the basis that consumers

[192] Ibid; also Sarocco supra n 42 12-13.

[193] Ibid. For a discussion on the different spam countering filter techniques see: ITU-T Series X: Data Networks, Open System Communication and Security (Cyberspace security countering spam) 'Interactive gateway system for countering spam' (Recommendation ITU-T X.1243 (12/2010) 5-9 http://www.itu.int/ITU-T/recommendations/rec.aspx?rec=10829 (date of use: 5 December 2015); for a framework for countering spam in IP based multimedia applications see ITU-T Series X: Data Networks, Open System Communications and Security (Cyberspace security countering spam) 'Framework for countering spam in IP based multimedia applications' (Recommendation ITU-T X.1245 (12/2010) 1-23 http://www.itu.int/ITU-T/recommendations/rec.aspx?rec=10830 (date of use: 30 November 2015). This document describes "IP multimedia spam" as "unsolicited messages or calls through multimedia applications which usually have special characteristics of spam such as bulkiness". Distinguished from traditional e-mail spam, IP multimedia indicates spam on communication methods over IP such as an instant messaging or voice over IP (VoIP) services (at 1); and for blocking spam as a counter measure see: ITU-T Series X: Data Networks, Open System Communications and Security 'Supplement on framework based on real time blocking lists for countering "VoIP spam" (ITU-T X.1245 Recommendation: Supplement 11 (09/2011) 1-18 at 3-9 http://www.itu.int/ITU-T/recommendations/rec.aspx?rec=11342 (date of use: 30 November 2015). This document notes 'VoIP spam' as "a kind of real-time voice spam emerging over VoIP services as telemarketing which includes communications with a telemarketer and interaction with the interactive voice response (IVR) system".

[194] Ibid.

[195] Ibid.

[196] Ibid.

[197] Ibid. ITU-T Series X 'Technologies involved in countering e-mail spam' supra n 184 1-19.

[198] ITU WSIS 'Curbing spam via technical measures: an overview' supra n 187 13.

are always themselves able to filter unwanted messages.[199] Furthermore, while some techniques successfully keep spam out of end users' inboxes, cost shifting continues once e-mail has entered an ISP or company network which would already have paid the price involved in handling the message.[200]

In conclusion, the ITU suggested that end-users, corporations, and ISPs must each play its part in curbing the scourge of spam.[201] Technical measures are a critical component in any multi-pronged strategy targeting spam, and if used in conjunction with other available measures, the tide in the war against spam can be turned.[202]

4.3.4.4 The establishment of industry partnership

The ITU noted that appropriate action on spam both nationally and internationally is necessary as part of a wider effort aimed at building confidence in the use of ICTs.[203] Role players such as industry ISPs, direct marketers, and software developers can contribute and also adapt their practices to combat spam.[204] This would be seen as a move towards promoting industry partnership in that most countries operate on a multi-national basis.[205]

Self-regulatory tools such as codes of conduct should also be encouraged and systematically improved by drawing on experience.[206] The sharing of expertise and best practices both across industry branches, and across countries and regions in the world, should be encouraged.[207] Improved cooperation on enforcement between industry and enforcement authorities also needs to be promoted, in particular, tracing spammers and providing evidence that can be used in investigation and prosecution.[208]

[199] Ibid.
[200] Ibid.
[201] Ibid.
[202] Ibid.
[203] ITU WSIS 'Multilateral and bilateral cooperation to combat spam' supra n 42 7.
[204] Ibid.
[205] Ibid.
[206] Ibid.
[207] Ibid.
[208] Ibid.

4.3.4.5 Consumer education

The ITU noted that user education is a necessary and ongoing component of an effective legal regime aimed at combating spam.[209] As users move onto the Internet they need to be educated on how to recognise and defeat tactics considered to be harmful by technical experts.[210] Users who are often the victims of spam are considered a part of the problem for two reasons: they read spam messages and also purchase items that are advertised through spam; they also enable spammers by failing to maintain adequate computer security.[211]

The ITU has noted that consumers in particular should be aware of the following: "the rules of the game; how to limit their exposure to spam; what filtering or basic security measures can be taken to minimise spam; and where to complain when confronted with spam".[212] Consumers are also advised to take the following into account in order to reduce the amount of spam that they receive: reduce posting on publicly accessible web sites;[213] create multiple e-mail addresses;[214] limit disclosure of e-mail addresses;[215] and use e-mail filters.[216]

[209] Rotenberg M 'Consumer perspectives on spam: challenges and challenges' (2004) 1-12 at 1 http://www.itu.int/osg/spu/spam/contributions/Background%20Paper%20consumer%20perspective%20on%20spam.pdf (date of use: 30 November 2015).

[210] Bambauer et al supra 42 33.

[211] Id 28-32. Regarding maintaining adequate computer security refers to those consumers who do not install and update proactive measures such as: firewalls, antivirus programs and spyware-detection software enable spammers to make use of their computers and Internet connections.

[212] ITU WSIS 'Multilateral and Bilateral cooperation to combating spam' supra n 42 8.

[213] Rotenberg supra n 209 1-3. It has been recommended that: "consumers avoid posting e-mail addresses on web sites so that their e-mail addresses cannot be obtained by various e-mail harvesting programs. While this is advisable it has been noted that consumers are routinely asked to provide e-mail addresses as part of a web site registration process. Furthermore, their e-mails are also posted on the Internet through chat and online services".

[214] Id 4-6. Organisations have proposed that "establishing e-mail accounts apart from personal addresses, be used for public disclosure or to receive marketing information and other junk mail. However, this has been found to be impractical in that consumers continue to find it difficult to protect their personal e-mail addresses and will also have to track multiple e-mail addresses in addition to the various privacy rules".

[215] Id 3-4. Consumers are advised to be aware "when filling out online forms or giving out e-mail addresses, of how those will be used. They are also advised to pay attention to checking boxes that request the right to send e-mails or to share their addresses with other parties. They are advised to opt-out if they are concerned about dissemination of their addresses".

[216] Id 3. Even though consumers have access to filters to block spammers who might attempt to infiltrate their mail boxes, "these, have however, been proven to be imperfect in that they either over-block or under-block the spam e-mails".

The role of education is also seen as of particular importance to the success of anti-spam legislation, with both national and international coalitions being formed to promote education.[217] At national level the following have been identified as playing an important role in consumer awareness:[218] action plans aimed at enhancing consumer education and awareness; and plans to promote international frameworks to fight spam. The ITU noted that there is however a lack of uniformity in anti-spam legislation in that spam is a major threat to consumer confidence, which in turn is a pre-requisite for the growth of e-commerce.[219] But that consumer education can help consumers identify privacy tools that may limit spam, but it remains an incomplete solution.[220] While user identification such as a sender's identity may reduce the risk of spoofing and phishing it is also said to increase privacy risks for consumers as personal information will be readily available.[221]

In conclusion, the ITU points out that education always succeeds only in part for the following reasons:[222] that users lack incentives to maintain perfect security as they do not gain the full benefit of measures they take to protect their computers; the reduction in the volume of spam they see bears little relation to these actions; and many users agree to host programs such as adware on their computers in exchange for free use of programs such as screensavers or peer-to-peer software.

4.3.4.6 International cooperation

The ITU noted that international cooperation on enforcement is essential for the following reasons: to ensure the effectiveness of anti-spam rules; to trace spamming activities; and to prosecute spammers regardless of where they are based.[223] The ITU encouraged countries to form partnerships aimed at combating spam.[224] The ITU noted

[217] Id 5-6.
[218] Ibid.
[219] Ibid.
[220] Ibid.
[221] Id 7.
[222] Bambauer et al supra n 42 33.
[223] ITU WSIS 'Multilateral and bilateral cooperation to combat spam' supra n 42 5.
[224] Id 7.

that as a pre-requisite national legislation should facilitate information sharing and mutual assistance between competent authorities in the different countries.[225] And that appropriate bilateral and/or multilateral cooperation would allow for information sharing and mutual assistance in specific cases of spam.[226] As a result a number of countries have entered into bi- and multilateral cooperation agreements by signing Memorandum of Understanding (MoU).[227] MoUs are not legally binding but they carry a degree of gravitas and mutual respect, are stronger than the so-called "gentlemen's agreements", and often represent a first step towards a legal contract.[228]

4.3.5 Conclusion

The ITU's work in combating spam is commendable. Not only has it called upon countries and organisations to work together to combat spam, it has also provided guidelines for those affected by this scourge. This research has revealed the challenges of having an anti-spam legislation in place. The ITU study on spam is a continuing one and member states are kept abreast of global developments in the field. In 2012 member states were again encouraged to take necessary measures to prevent the propagation of unsolicited communications and to minimise its impact on international telecommunication services.[229] In 2013 an ITU workshop on countering and combating

[225] Ibid.

[226] Ibid.

[227] Hereafter referred to as 'MoU'. An MoU is "a formal agreement between two or more parties which can be used by companies or organisations to establish official partnerships. These MoUs are popular in multinational international relations, because unlike a treaty they are quickly ratified and can be kept confidential". WhatIs.com 'Memorandum of understanding (MOU or MoU)' http://whatis.techtarget.com/definition/memorandum-of-understanding-MOU-or-MoU (date of use: 5 December 2015). Countries that have signed these MoUs include USA, Australia, and South Korea to name but a few. Some of these MoUs will be highlighted when the anti-spam laws of a particular country are discussed in Chapters 6 and 7 below. See ITU WSIS 'Multilateral and bilateral cooperation to combat spam' supra n 42 1-8. For a general discussion of some of these agreements see ITU-T Series X: Data Networks, Open System Communications and Security ITU-T X. 1240 Series Supplement on Countering Spam and Associated Threats (Supplement 6) (09/2009) http://www.itu.int/ITU-T/recommendations/rec/aspx?rec=10245 (date of use: 30 November 2015).

[228] WhatIs.com 'Memorandum of understanding (MOU or MoU)' http://whatis.techtarget.com/definition/memorandum-of-understanding-MOU-or-MoU (date of use: 5 December 2015).

[229] See article 5B of the International Telecommunications Regulation dealing with unsolicited bulk electronic communications 'Final Acts World Conference on International Telecommunications' (Dubai 2012) http://ww.itu.int/en/ITU-T/Workshops-and-Seminars/spam/201307/pages/

spam was held in Durban, South Africa.[230] The workshop noted that while there is no single solution to combating spam, in practice there are various complementary approaches to the problem which have proved practical.[231] It was also noted that the problem of spam affects developed and developing countries alike, and that each of these parties need the other if spam is to be successfully combated.[232] Partnerships and/or agreements between the African Union (AU) and the African Telecommunications Union (ATU) should be formed, together with the ITU and Internet Society (ISOC). The need for a follow-up report was mooted.[233] In 2014 the ITU and ISOC held discussions on the tools available and the role of collaboration in combating the threats posed by spam.[234] It was noted that legislation is not in place in certain developing countries even though they share the problem of spam with developed countries and are also active in spamming activities.[235]

It remains to be seen how the ITU's work will proceed beyond 2016. In the meantime countries with anti-spam laws in place and those without such laws must seriously consider the guidelines set out above as regards their national laws. At a global level these countries should also consider a set of international standards on acceptable ethics, the development of best practices, and technical assistance in this area. Below follows the discussion on how the OECD is combating spam.

default.aspx (date of use: 30 November 2015). At the time of writing there were 89 signatories to these Final Acts, South Africa being one. Since then the ITU Council Working Group on International Internet-related Public Policy Issues (CWG-Internet) has held open consultations with all stakeholders invited to provide input on the international public-policy issues related to effectively countering and combating spam.

[230] ITU 'Workshop on countering and combating spam' (Durban South Africa 8 July 2013) http://www.itu.int/en/ITU-T/Workshops-and-Seminars/spam/201307/Pages/default.aspx (date of use: 30 November 2015).

[231] Ibid.

[232] Ibid.

[233] ITU 'Workshop on countering and combating spam' supra n 230. These partnerships will be discussed in the next chapter when regional initiatives for combating spam are considered.

[234] ITU WSIS 'WSIS+10 High Level Event' (Geneva 10-13 June 2014) http://www.itu.int/net/wsis/implementation/2014/forum (date of use: 5 November 2015). This event was designed to review progress made in the implementation of the WSIS outcomes under the mandates of participating agencies, and to take stock of achievements in the last ten years based on reports of WSIS stakeholders.

[235] Ibid.

4.4 The OECD

4.4.1 Background

The OECD was formed in 1961 with the aim of promoting policies to improve the economic and social well-being of people around the world, and providing a forum in which governments can work together to share experiences and seek solutions to common problems.[236] Headquartered in Paris, France, the OECD currently has 34 members.[237] In 2011 the OECD turned 50 and adpoted as its mandate going forward: to restore confidence in markets and institutions and to re-establish healthy public finances as a basis for future sustainable economic growth.[238]

4.4.2 The OECD's initiatives in combating spam

4.4.2.1 Task Force on spam

The OECD appointed a Task Force which included participants from member states and other stakeholders, to take the lead in developing an anti-spam toolkit.[239] The Task Force was given two years (from the time the mandate was granted) to study existing and emerging anti-spam strategies across all sectors and to develop and promote the toolkit focused on practical anti-spam strategies, arrangements, and solutions.[240] It was

[236] OECD 'About the OECD' http://www.oecd.org/about (date of use: 30 November 2015). The OECD was preceded by the Organisation for European Economic Co-operation (OEEC) which was established on 16 April 1948. See OECD 'Organisation for European Economic Co-operation' http://www.oecd.org/general/organisationforeuropean economicco-operation.htm (date of use: 9 December 2015).

[237] In May 2007 the OECD Council at Ministerial level adopted a resolution to strengthen the co-operation with South Africa as well as Brazil, China, India and Indonesia through a program of enhanced engagement. Thus making South Africa one of the many non-member economies with which the OECD has a working relationship. See OECD 'OECD invites five countries to membership talks, offers enhanced engagement to other big players' http://www.oecd.org/southafrica/southafricaandtheoecd.htm (date of use: 9 December 2015).

[238] See Meeting of the OECD Council at Ministerial Level 'OECD 50th Anniversary Vision Statement' (C/MIN(2011)6 1-4 http://www.oecd.org/mcm/48064973.pdf (date of use: 9 December 2015).

[239] Other stakeholders included the European Commission, the Business Advisory Committee to the OECD, and civil society. OECD 'OECD launches anti-spam toolkit and invites public contributions' http://www.oecd.org/internet/ieconomy/oecdlaunchesanti-spamtoolkitandinvites publiccontributions.htm (date of use: 30 November 2015).

[240] Ibid.

also mandated to devise a public awareness strategy to support global efforts to combat spam.[241] The Task Force's initial mandate was to decide on appropriate action to be taken and the roles of the different stakeholders in fighting spam.[242] The OECD agreed that governments should establish clear national anti-spam policies in concert with other players,[243] collaborate with the private sector, and also promote cross-border cooperation.[244] It also noted that in order to fight spam it was important to set-up domestic coordination groups and create appropriate regulatory frameworks based on well-defined policy objectives backed by effective enforcement mechanisms.[245] In response, the Task Force developed the concept of the anti-spam toolkit to provide OECD member states with a comprehensive policy orientation and consistent framework in their fight against spam. This was also to be applicable to and useful for non-OECD countries.[246]

4.4.2.2 The Anti-spam Toolkit

Like the ITU, the OECD noted that there was no simple solution to eliminate spam but that measures should be taken to prevent it. Those measures should be designed to meet a number of policy goals and objectives.[247] The toolkit contains recommendations to assist policy makers, regulators, and industry players orient their spam policies and restore trust in the Internet and e-mail.[248] The toolkit includes a spam regulation handbook (a reference guide) to different existing approaches to spam regulation in order to help identify loopholes and ways of improving international enforcement and cooperation.[249]

[241] OECD 'Report of the OECD Task Force on spam: Anti-spam Toolkit of recommended policies and measures' 2 (DSTI/CP/ICCP/SPAM(2005)3/FINAL) http://www.oecd.org/internet/consumer/36494147.pdf (date of use: 30 November 2015). Hereafter 'Anti-spam ToolKit'.

[242] Id 6.

[243] Ibid. This is consistent with the ITU, see para 4.3.4.2 above.

[244] Ibid.

[245] Ibid.

[246] Id 7.

[247] These policies and objectives include: to preserve the benefits of electronic communication; to prohibit and apply sanctions against the act of spamming as defined by national laws; and to reduce the amount of spam. See the Anti-spam Toolkit supra n 241 6.

[248] Ibid.

[249] See OECD 'OECD launches anti-spam toolkit and invites public contributions' supra n 241.

It also provides for an examination of self-regulation arrangements which exist at industry, national, or international levels which can be applied to fight spam.[250] An analysis of existing and emerging counter-spam technical measures, including authentication technology, is included in the toolkit.[251] It further includes a central information resource to educate members and raise awareness of the threat of spam and how to fight it.[252] An overview of existing partnerships against spam, examples of good practice, and lessons that can be learned for the development of cooperative anti-spam partnerships are also included.[253] The aim of the toolkit is to provide OECD members with a comprehensive policy orientation and consistent framework in their fight against spam.[254] This toolkit contains eight elements to assist member states to implement spam laws in their regions.

4.4.2.3 Eight elements contained in the Anti-spam Toolkit

The toolkit comprises of the following eight elements which are discussed separately below: anti-spam regulation; anti-spam enforcement; industry-driven initiatives; anti-spam technology; education and awareness; cooperative partnerships against spam; and spam quantification; and global cooperation or outreach.

(a) Anti-spam regulation

The OECD indicated that national anti-spam legislation which tackles spam and related problems is fundamental and should preserve the benefits of electronic communications.[255] National legislation should also prohibit and take action against spamming as defined by a state's national law, and act to reduce the amount of

[250] Ibid.
[251] Ibid.
[252] Ibid. This includes tips for users on how to protect themselves from spam and how to avoid phishing when spammers fake e-mails to encourage Internet users to divulge confidential financial data.
[253] Ibid.
[254] Ibid.
[255] Anti-spam Toolkit supra n 241 8.

spam.[256] In pursuing these goals law makers should consider four general principles: policy direction; regulatory simplicity; enforcement effectiveness; and international linkages.[257] In reviewing best practices for legislation the following elements should as far as possible be included, account being had to a country's institutional and legal framework.

Services concerned

This element concerns the definition of spam as focusing on a particular medium, or attempting to provide a technology-neutral approach.[258] In developing an anti-spam regulatory approach policy makers should consider that with the convergence of messaging formats made possible by the emergence of new technologies and applications, new and unforeseen messaging media arise.[259] New legislation should therefore be sufficiently flexible to ensure that future communication technologies are covered in the event of their being subject to new forms of spam.[260] At the same time it should be recognised that any policy or regulatory regime imposed on a messaging technology will have an impact on both legitimate messaging and the spam messages being targeted.[261] The nature of spam messages is aimed at making money through the sale of goods and/or services such as, for example, religious or political non-commercial messages.[262] However, limiting the scope of spam legislation to commercial messages may result in legitimising equally harmful types of spam.[263]

[256] Ibid.

[257] Id 8, 24-5. The OECD notes that "legislation should be in a position to provide a clear policy direction, and that the main lines and objectives of national and international anti-spam policy should be outlined at an earlier stage. 'Regulatory simplicity' means legislation should be simple and short; enforcement effectiveness has been noted a fundamental issue which if not dealt with appropriately can make a good piece of legislation useless. Therefore, it is important to put in place an effective sanction regime and appropriate standards of proof, and also that appropriate powers and resources need to be allocated for 'enforcement authorities'; and "international linkages" involves the possibility of legislation for-seeing appropriate international linkages and providing national authorities with the possibility to co-operate in investigations and exchange information with foreign authorities".

[258] Anti-spam Toolkit supra n 241 9 and 26.

[259] Id 26. These new technologies and applications include the 3G and 4G or VoIP.

[260] Ibid.

[261] Ibid.

[262] Id 9 and 26-7. Only messages with commercial content and not the volume.

[263] Ibid.

Consent

A fundamental principle used in formulating most anti-spam policy frameworks is based on ensuring that suitable consent is obtained from potential message recipients before sending commercial messages.[264] This type of consent focuses mainly on the mechanisms used in anti-spam legislation to protect consumers, namely the opt-in and opt-out mechanisims.[265] The OECD noted that while the opt-in versus opt-out mechanism debate was appropriate in the past, recent approaches to spam regulation have incorporated more complex and subtle methods involving consent.[266]

Information on message origins

The OECD observed that while appropriate legislation and effective enforcement are essential, governments should also raise awareness among consumers of the possible risks they (consumers) can be exposed to in using e-mail and educate users on how to recognise spam e-mail.[267] If the sender disguises its header information it makes it very difficult for an enforcement agency to identify the spammer, and it also makes an

[264] Id 9 and 27-8.

[265] See the discussion on these two mechanisms in para 4.3.4.2 (c) (ii) above.

[266] See Anti-spam Toolkit supra n 241 9 and 27-8. The OECD defines the following types of consent: "express consent", which is "a direct indication from the person one wishes to contact that it is in order to send the messages. Consent can be given in a variety of ways such as: filling in a paper form; ticking a box on a web site; and during a phone call or face to face conversation. The advantage of this type of consent is that a user's privacy is protected so ensuring greater control of personal data. The burden of proving express consent lies with the sender of the message and not with the recipient. The disadvantage of express consent is the difficulty businesses have keeping records of such consent. This results in the restriction on a potential pool of recipients who can be targeted for legitimate mail should those records not be available"; "Inferred" and "implicit consent" is consent which generally "can be inferred from the recipient's conduct and/or other business relationships. While the advantage of this consent is that it is more flexible, the disadvantage is that it may be difficult to define when a message can be related to an existing business relationship"; "Assumed consent" is "consent which presumes that consent is provided until the recipient withdraws, for example by un-subscribing from a mailing list or by placing the electronic address on a do-not-contact list. The advantage of this type of consent is that it is less constricting to the operation of online commerce, in that there is minimal risk of inadvertently proscribing legitimate messaging. It also does not restrict choice of e-mail recipients who might receive commercial messages. The disadvantage is that assumed consent transfers the burden of effort and cost to the consumer – to unsubscribe from a mailing list the e-mail must be opened and responded to. This is contrary to good e-security practice unless the e-mail is from a known and trusted source. Unsubscribe links are often non-functional which places the evidentiary burden on recipient of the message".

[267] Id 30.

investigation complex, expensive, and time consuming.[268] In addition, technical instruments should be developed to support legislative efforts and the development and implementation of e-mail authentication solutions.[269]

Ancillary elements

These ancillary elements include issues such as the prohibition of harvesting software and harvested address lists and the use of dictionary attacks.[270] The OECD notes that an additional sanction should be imposed if such tools are used to aid the sending of spam in contravention of an anti-spam legislation.[271] In this instance sanctions should apply not only to the person actually sending the spam, but also to the commissioning or authorisation of the spamming.[272] This should further extend to other entities that benefit from the spamming and who normally share the resulting profits.[273]

(b) Anti-enforcement

The OECD pointed out that legislation needs to ensure that enforcement agencies have adequate powers to function effectively.[274] In furthering their work to facilitate anti-spam legislation across borders, governments may need to intervene in the following areas: national coordination; procedures and sanctions; empowerment of enforcement authorities; and cross-border enforcement cooperation.

National coordination

[268] Ibid.

[269] Ibid.

[270] Ibid. Also see para 4.3.4.2 (c) (iv) above.

[271] See Anti-spam Toolkit supra n 241 30-1.

[272] Id 31-6.

[273] Ibid. Other elements include: "(a) cyber-crime and content-related questions which include illegal access to computers via zombie computers, or using third-party resources to send spam; misleading or fraudulent content (e-mail used as a form of scam or misleading trade practice, and also security threats such as the use of malware, viruses et cetera); and (b) labelling, cross-border issues, identification of involved parties (eg, users and ISPs)".

[274] Id 11.

Spam impacts not only on consumer rights and data privacy, but also on network security and efficiency. The OECD noted that countries have different agencies with different powers and priorities mandated to deal with one or more aspect of spam.[275] Some countries may need to increase efforts to strengthen an agency as a contact point for foreign authorities to facilitate cross-border cooperation.[276] To support these initiatives the OECD has set up a list of "contact points for authorities" to facilitate cross-border cooperation.[277]

Empowerment of enforcement authorities

The OECD noted that since the evidence of illegal spam is generally electronic and may be stored on many individual computers, devices, or networks in multiple countries or jurisdictions, enforcement authorities dealing with spam need appropriate powers to preserve, access, intercept, search, and seize electronic evidence.[278] Evidence gathering in this instance should be broader than just records of message transmission, as financial records and related correspondence can potentially assist in determining who commissioned or otherwise generated the spam.[279]

Procedures and sanctions

The OECD noted that legislation must make provision for severe sanctions and discourage spam by implementing criminal sanctions.[280]

[275] Id 37.

[276] Ibid.

[277] Id 37-8.

[278] Ibid.

[279] Ibid.

[280] Id 38-9. The following remedies are available to OECD member countries. "Civil proceedings which include monetary sanctions like a civil fine which might be an amount to be determined depending on the nature and extent of violations; consumer redress; non-monetary sanctions; warning letters; and injunctions which can be brought by private citizens, public and private enforcement agencies, and ISPs; criminal proceedings which may result in a fine, non-monetary sanction, and imprisonment. While this is perceived as a strong remedy – especially when the content of spam is criminal or when the spammer has not complied with an administrative order – it is time consuming and carries a higher burden of proof; and administrative action, for example monetary sanctions, administrative fines, non-monetary sanctions, injunctions, and warning letters". The OECD also noted that administrative fees and non-monetary sanctions are the primary instruments for

Cross-border enforcement cooperation

Enforcement action across borders would benefit from a global strategy to overcome a number of challenges, most notably information gathering and sharing.[281] The OECD adopted the following guidelines to improve cross-border cooperation:[282] the establishment of a domestic framework to empower national enforcement authorities to investigate and take action against spammers or the dissemination of spam; and the improvement of the ability of authorities to cooperate with their foreign counterparts by authorising national bodies to share relevant information and provide investigative assistance.

(c) Industry-driven initiatives

The OECD recommends that in order to deal appropriately with spam, the anti-spam laws in countries must be linked to self-regulatory initiatives undertaken by private-sector players such as ISPs, telecommunication operators, direct marketers, online operators, software companies, and their associates.[283] The OECD noted that ISPs play an important role in the field of Internet security and the idea that messaging providers should intervene actively to prevent spam from being sent from or across their networks, is gaining acceptance.[284] But it also notes that there are generally no provisions in national legislative instruments which place any kind of obligation on ISPs to intervene actively to help eliminate spam.[285] However, most ISPs are noted as having a commercial interest in blocking or limiting incoming spam to protect their customers

enforcement authorities in many countries. The application for administrative remedies avoids the necessity of going through the civil or criminal courts".

[281] Id 41.

[282] Ibid. Other guidelines includes: to improve procedures for cooperation, prioritise requests for assistance, to make use of common resources and networks, and to develop new cooperative models between enforcement authorities and relevant private sector entities.

[283] Id 11-12 and 42.

[284] Id 42-5.

[285] Ibid.

should any massive influx of spam disrupt their service and affect both their availability and reliability.[286]

(d) Anti-spam technologies

Regarding anti-spam technologies, the OECD pointed out that what is required is defensive technology that goes beyond text-based tools to tools that analyse behavioural and contextual factors to determine whether to accept or reject specific mail or even attempted connections.[287] The types of anti-spam technology would include: authentication of electronic mail;[288] a Sender Policy Framework (SPF); sender identification;[289] and blacklists and whitelists.[290]

(e) Education and awareness

The OECD noted that a comprehensive anti-spam strategy must take the end-user who is the recipient of the spam into account.[291] The recipient is also the potential victim of viruses and scams, yet is also the person who has control over his or her computer and personal information.[292] Users still do not perceive security as a real issue as they are not aware of the risks connected with their activities when surfing the Internet.[293] Education and awareness strategies should target the role players identified below.

[286] For a discussion of other stakeholders such as banks, operators, and industry associates see: id 41-8.

[287] Id 13 and 49-61 for a discussion of these technologies.

[288] Id 50. “Mail authentication methods fall into the category of rules (which although they help in the fight against spam), do not constitute specific anti-spam technologies. While perpetrators use identification cards, these are not trust markers but help with the requirement of transparency which will be of greater benefit to legitimate senders than spammers”.

[289] Id 51. “The proliferation of spam may be ascribed to the ability of spammers to hide their true identity by masking headers et cetera. With the use of sender authentication the burden would then be placed on the sender of spam rather than on the receiver, and would render phishing attacks more difficult. SPF and sender ID can be best used to test whether an e-mail server is authorized to send on behalf of a given domain. This is done by publishing a record in the Domain Name System (DNS) which lists the authorized e-mail servers for a domain. The two techniques differ in the choice of the identity tested” (ibid).

[290] Id 52-3.

[291] Id 13-14 and 62.

[292] Ibid.

[293] Id 14 and 63.

Individual users and governments

The OECD noted that governments are urged to develop public information and awareness campaigns to educate end-users on the products and services they are using and the associated risks they may face.[294] This information will enable users to protect themselves from spam, viruses, and other malicious codes.[295] Governments should also organise nation-wide campaigns to attract the attention of the media and the population at large.[296] They also need to work with the private sector, civil society, and other interested parties on user education campaigns and other initiatives.[297]

Government enforcement agencies should partner with industry and consumer groups to educate users and promote information sharing.[298] Government, should also cooperate with the private sector to promote the development of technological tools to fight spam, including tools to facilitate the location and identification of spammers.[299]

ISPs, and other network operators

The OECD noted that ISPs and other network operators, including mobile operators, need to use their company-customer communication channels (web site, portals, SMS, newsletters) to provide pertinent information to their customers.[300] The information should include how recipients can avoid spam and risks connected with spam e-mails, SMS, MMS; what anti-spam and anti-virus filters and open source solutions are available to the platform concerned; an indication of how to report spam abuses to ISPs or users, operators and competent authorities; and e-mail or phone contact to the provider's abuse desk.[301]

[294] Id 13.

[295] Ibid.

[296] Ibid.

[297] Ibid.

[298] Id 63.

[299] Ibid.

[300] Id 13.

[301] Ibid.

User groups

The OECD notes that user groups (including children, students, and senior citizens) can be targeted with information tailored to their needs/interests.[302] The following is recommended to these groups: computer classes for senior citizens are seen as the best way in which to introduce the concept of computer and information security;[303] for children and students, awareness of online threats and security issues should be part of their educational curriculum;[304] and schools should include sessions on spam in their computer courses and also address issues such as online fraud, viruses, illegal content, and on-line/computer/Internet etiquette.[305]

Users and phishing

The OECD notes that a solution for users will include the implementation of technical measures to limit the phishing and reduce the consequent damages.[306] Online operators should establish, implement, and enforce appropriate and clear policies on e-mail practices with their customers, and also develop consumer education initiatives.[307] Awareness campaigns are essential in educating individuals on how to recognise and respond to deceptive and fraudulent messages.[308]

Companies: Small, medium, and large enterprises

[302] Ibid.

[303] Ibid.

[304] Id 63.

[305] Ibid. Parents are also urged to play an important role in teaching children how to be safe online by making them understand the risks of online communications and how to protect themselves.

[306] Id 64.

[307] Ibid.

[308] Ibid. The OECD noted that "government authorities, online operators, and ISPs were at that time developing educational tools for users. The following provisions should be stressed when dealing with this aspect: instruct users receiving an e-mail(s) asking for personal information to call the company directly to ask for confirmation or type in the company's web address, while avoiding clicking on the link provided in the e-mail; advise users to utilise anti-virus software and firewalls to protect their computers and avoid accepting unwanted files that could harm the computer or track a consumer's internet activities; and warn users against e-mailing personal or financial information".

Companies usually fall victim to spam and malware because their e-mail addresses are accessible from public sites or are widely circulated.[309] The OECD noted that educational needs of large companies will be different from those of small or medium-sized companies.[310] Large companies are urged to make available to their staff pamphlets explaining the company's e-mail security policy and existing filters and best practices for dealing with spam.[311] Small and medium enterprises (SMEs), on the other hand, need to provide their employees with specific information on simplified security management practices, training material, software, et cetera.[312] Regulators and business associations can play an important role in educating companies by disseminating information on how businesses can communicate with its clients using e-mail, for example – in a way that complies with national legislation.[313]

Direct marketing associations

Direct marketing associations should inform their members of relevant anti-spam legislation in force in the message's country of origin and country of destination.[314] In order to assist direct marketers in this endeavour, the Direct Marketing Association (DMA) provides lists of online marketing best practices, often in the form of checklists indicating the requirements a company must satisfy from the moment it decides to launch an online advertising campaign, to the actual sending of the message.[315]

(f) Cooperative partnership against spam

The OECD noted that issues such as spam and cyber security are affecting public and private players. Both therefore share a common interest in preserving the availability and reliability of communication tools to promote the development of the digital

[309] Ibid.
[310] Ibid.
[311] Id 65-6.
[312] Ibid.
[313] Id 14.
[314] Id 14 and 66.
[315] Ibid.

economy.[316] These partnerships include a government-led regulatory approach, where the regulator sets the rules which impose certain responsibilities on private companies – for example, the obligation to apply security practices to the more market-led approach in which private operators autonomously decide their level of involvement and participation.[317]

Public and private sectors have also developed a number of innovative ways in which to cooperate because governments also seek the involvement of both private sector entities and non-governmental bodies in the discussion of comprehensive anti-spam strategies and activities.[318] As a rule, the objectives of strategic partnership are to improve networking awareness, raise activity, and share information.[319] More operational partnerships also contribute to education, development (and application) of best practices, and the exchange of information and data on cross-border cases of spam.[320]

The OECD further noted that private-public partnerships in the field of spam are necessary to promote interaction and cooperation between the two players, especially considering the wide range of stakeholders involved and their different needs and backgrounds.[321] Relying solely on legislation to impose obligations on private players would not be effective unless combined with other measures, an example being that laws cannot keep up with technical change.[322] If widely applied, best practices can be effective when combined with legal and other measures. In this context strategic partnerships such as those between different task forces created at national and international levels, are a fundamental tool in the improvement of communication, understanding of reciprocal needs, expectations, and problems.[323] They therefore

[316] Id 66; also para 4.3.4.4 above.
[317] Ibid.
[318] Id 67-8.
[319] Id 67-9.
[320] Id 67.
[321] Id 68.
[322] Ibid.
[323] Ibid.

promote further cooperation and mutual involvement.[324] For partnership to succeed and achieve concrete results, which can then be put into practice by the different stakeholders, the following elements as noted by the OECD appear necessary: a commitment and real contribution from all parties (ownership of the end product);[325] and well-defined objectives and timeframes.[326] National partnerships that feed into international initiatives and partnerships are needed to complement and harmonise solutions.[327] Rather than duplicating efforts, partnerships should build on tried and trusted existing relationships and representative bodies.[328]

(g) Spam statistics

The OECD noted that most of the data on spam originates from industry, in particular from anti-spam solution providers and also from ISPs.[329] Data gathered by these players is difficult to compare as they relate to different user bases and are founded on different parameters.[330] Filtering companies and ISPs (using filters) collect data from their customers that provide information on the amount of spam detected by the filters.[331] This data gives an indication of the growth of spam relative to the total volume of e-mail traffic (different possible content) and affected countries.[332] Statistics can also provide relevant information for policy makers on the burden that spammers impose on network operators.[333]

(h) Global cooperation (outreach)

[324] Ibid.

[325] Ibid.

[326] Ibid.

[327] Ibid.

[328] Ibid.

[329] Id 14-15 and 70-2.

[330] Ibid.

[331] Ibid.

[332] Ibid. Data on spam is, to a limited extent, also collected by some government or public organisations which have the responsibility to develop anti-spam policies or regulations.

[333] Ibid.

The OECD noted that global cooperation has two main objectives namely: to promote appropriate domestic frameworks to counter spam; and to encourage cooperation among countries, the private sector, civil society, and other stakeholders.[334] Cooperation ensures that the problem of spam is addressed comprehensively and promotes the harmonised and widespread application of technical measures and the effective enforcement of applicable rules.[335] The OECD also encourages its member states to contribute to the development of laws and regulation and enforcement measures; to promote education on all levels; and to facilitate industry cooperation.[336] The OECD is also involved in outreach activities such as contributing to anti-spam initiatives at the global level in partnership with other organisations active in the field.[337] It also promotes cooperation and the exchange of information and facilitates the dissemination of its anti-spam toolkit by the task force to provide education, regulatory and technical measures, and a contact list of enforcement authorities and anti-spam legislation around the world.[338]

4.4.3. Conclusion

As noted by the OECD, all stakeholders have an important role to play in fighting spam. Governments can contribute by: (a) establishing clear national anti-spam policies in concert with other players; (b) collaborating with private operators and promoting cross-

[334] Id 15 and 73.

[335] Ibid.

[336] Id 74. Regarding law and regulation enforcement, the OECD noted that “international co-operation in the field of law and regulation is fundamental to support the establishment of an appropriate anti-spam regulatory framework in all countries, possibly following a set of basic harmonised principles at the international level. National policy should include measures to facilitate international cooperation and the sharing of information and practices. Educational and awareness tools which have already been developed should be made available more generally to all users, operators, schools, and public authorities in all countries. Considering that in developing countries Internet access is often collective – for example, users connect from work, schools, and Internet cafés – this information should also be made available at those places. The OECD also noted that establishing a series of best common practices is a global objective and that all ISPs should be involved. The commitment of industry will be necessary for further steps – in particular international co-operation would be useful – to bring together ISPs from developed economies which have considerable experience in the field and their counterparts in developing economies in order to share knowledge, experience and best practices”.

[337] Ibid. This includes support for developing countries from those technically developed countries and the international community in facing the problem of spam and Internet security.

[338] Ibid.

border cooperation; (c) setting up domestic coordination groups; and (d) creating appropriate regulatory frameworks based on well-defined policy objectives and backed by effective enforcement mechanisms which can greatly contribute to the anti-spam battle.[339]

On the basis of this framework it is hoped the private sector will take the lead in the development of relevant business practices and innovative technical solutions that can contribute to the education of users.[340] Coordination beween private and public players is crucial to the achievement of results in the fight against spam.[341] In considering the rapid pace of technical evolution and changing fraudulent and illegal online practices, the anti-spam toolkit is seen not as a tool for providing answers, but rather as a tool for policy orientation.[342] As spam is not a problem that will "go away" once the task force has fulfilled its mandate, it is important to establish and maintain a clear strategy for fighting spam through continuing national coordination and public/private cooperation and dialogue.[343]

4.5 Commentary and conclusion on ITU and OECD initiatives

The contributions of the ITU and OECD illustrate that spam affects a number of stakeholders, it can be combated only through a multi-pronged approach. It is important to note that the work of these two organisations in combating spam compliment one another. In their documentation – surveys, reports, the toolkit – each has outlined what a multi-pronged approach should entail by providing guidelines on how to implement recommendations outlined above in the respective regions.

Both the ITU and the OECD noted that whether spam is regulated in a single or in multiple pieces of legislation, the crucial consideration is that the provisions dealing with the basic elements identified be included in that legislation. Countries can benefit from

[339] Ibid.
[340] Ibid.
[341] Ibid.
[342] Ibid.
[343] Ibid.

these guidelines to strengthen their enforcement regimes. Both the ITU and OECD notes that spam has survived all regulation, technical measures, or other obstacles thrown at it, and therefore an on-going study is necessary, and, it is hoped, will lead to a solution in the future. It was noted that spam is as much a problem in developing as in developed countries. However, given certain technical issues it has also been noted that much-needed assistance is long overdue to ensure that developing countries are also equipped to fight spam.

Perhaps the most important element in the multi-pronged approach is that of involving the users themselves. Both organisations laid down guidelines as to who should be responsible for educating consumers and how this should be achieved. Education starts with consumers themselves monitoring their online activities and taking care as to whom they reveal their personal information. ISPs also have a prominent role to play as they are best equipped to protect users. By educating users ISPs will also be assisting in minimising the majority of the problems they run into in attempting to protect their users.

As spam is also a global problem, a further challenge is to ensure that national laws are harmonised, especially as regards issues of enforcement and collaboration between countries is therefore necessary to ensure that this battle is won both locally and globally. However, all this is possible only if each and every stakeholder involved does its part in combating this scourge. Partnerships should therefore include agreements between countries themselves, or between organisations within a particular country and other organisations beyond borders in order to combat spam.

While these are all guidelines and so not compulsory, it remains to be seen if those countries that do not have anti-spam laws in place will adopt legislation reflecting the guidelines laid down by both the ITU and OECD. Countries that already have anti-spam laws in place, also have an opportunity to improve their laws.

Having outlined the international arena’s contribution to this issue, regional initiatives aimed at combating spam will be discussed in the next chapter.

CHAPTER 5

REGIONAL INITIATIVES TO COMBAT SPAM: AFRICAN REGION

5.1 Introduction

In the previous chapter an outline of international initiatives to combat spam was presented. In this chapter focus is on regional initiatives. A number of regions in the world have contributed, and continue to contribute to initiatives aimed at combating spam.[1] The African region and its initiatives will be the main focus. The study is undertaken because Africa is in the process of harmonising its ICT laws. South Africa as a part of this region is also involved as these initiatives affect it either directly or indirectly.

When dealing with Africa it is important that the following initiatives are considered: The African Union's (AU) contribution to the issue of spam and developments in part of its regional communities namely: The Common Market for Eastern and Southern Africa (COMESA); and the Southern African Development Community (SADC). In addition, account must be had of the role of the African Telecommunications Union (ATU). The discussion centers on the background to the specific groupings; their initiatives, with specific reference to the instruments developed to combat spam; and lastly, a commentary on those particular instruments. In conclusion, a contexualisation of the regional initiatives to combat spam is addressed in order to highlight both harmonised approaches and areas in which harmonisation is yet to be achieved.

5.2 African Region

5.2.1 Background

[1] These include among others: the European Union (EU), see European Union 'The history of the European Union' http://www.europa.eu/about-eu/eu-historyy/index_en.htm (date of use: 09 December 2015). For a discussion of the EU's spam regulation see Geissler *Bulk Unsolicited Electronic Messages* 1-403; Asia Pacific Economic Cooperation 'History' http://www.apec.org/About-Us/About-APEC/History.aspx (date of use: 9 December 2015), and Association of Southeast Asian Nations (ASEAN) 'History: the founding of ASEAN' http://www.asean.org/asean/about-asean/history (date of use: 9 December 2015).

Africa is one of the six continents in the world and consists of 54 countries made up of different ethnic groups, cultures, traditions, language et cetera. For the past five hundred years Africa has been plagued by misfortune and injustice resulting from colonial rule.[2] Africa, as a whole, broke free of its Colonial shackles only during the late 1950s and early 1960s. With independence came the major project of rebuilding the states, a process which continues to this day.[3] This new dawn for Africa was heralded by the establishment of the Organisation of African Unity[4] in 1963, which has since been renamed by the African Union.[5]

5.2.2. African Union

The establishment of the AU is a signal event in the institutional evolution of the continent.[6] In July 1999, the OAU Heads of State and Governments issued a declaration calling for the establishment of an AU.[7] The AU aimed to accelerate the process of integration on the continent[8] and enable Africa to play its rightful role in

[2] See South African History Online 'The impact of colonialism' http://www.sahistory.org.za/topic/impact-colonialism (date of use: 27 December 2015); and Iweriebor EEG 'The colonisation of Africa' http://exhibitions.nypl.org/africanaage/essay-colonisation-of-africa.html (date of use: 27 December 2015).

[3] The year of Africa's independence is noted as 1960, the year in which most of the sub-Saharan African nations, including fourteen former French colonies gained independence from their colonisers. See France24 '1960: The year of independence' http://www.france24.com/en/20100214-1960-year-independence (date of use: 27 December 2015); also Japan African Network 'African countries' independence days' http://www.japanafricanet.com/directory/ presidents/africanindependence.html (date of use: 27 December 2015); and Talton B The challenge of decolonization in Africa http://exhibitions.nypl.org/africanaage/essay-challenge-of-decolonization-africa.html (date of use: 27 December 2015).

[4] Hereafter referred to as 'the OAU'. The OAU was established on 25 May 1963 in Addis Ababa, Ethiopia. The OAU Charter was signed by representatives of 32 governments. Department of International Relations and Cooperation (RSA) 'Organization of African Unity (OAU)/African Union (AU)' http://www.dfa.gov.za/foreign/Multilateral/africa/oau.htm (date of use: 9 December 2015). For a background on the OAU and its transformation see Bujra A 'Africa: The transition from OAU to AU' Lecture delivered at ACARTSOD Tripoli, Libya (23 September 2002) http://www.dpmf.org/meetings/From-OAU-AU.html (date of use: 9 December 2015), and Du Plessis M 'The African Union' in Dugard J *International Law: A South African Perspective* 3 ed (Juta & co, Ltd Lansdowne SA 2006) 546-54.

[5] Hereafter referred to as 'the AU'. The AU was established in 2002 by the nations of the former OAU. See Infoplease 'African Union' http://www.infoplease.com/encyclopedia/history/african-union.html (date of use: 3 March 2017); and African Union Summit 'Transition from the OAU to the African Union' http://www.au2002.gov.za/docs/background/oau_to_au.htm (date of use: 3 March 2017).

[6] African Union 'AU in a nutshell' http://www.au.int/en/about/nutshell (date of use: 9 December 2015) for a background history of the AU.

[7] Ibid.

[8] Ibid.

the global economy while addressing multifaceted social, economic, and political problems compounded by negative aspects of globalisation.[9]

The AU's objectives[10] are, among others, "to achieve greater unity and solidarity between African countries and the peoples of Africa; to harmonise the policies between the existing and future regional economic communities for gradual attainment of the objectives of the Union; and to advance the development of the continent by promoting research in all fields but particularly in science and technology". There are 54 countries which form part of the AU, and until recently only one was not a member namely: Morocco.[11]

5.2.3 Regional integration in the African region

The African region currently has eight regional communities, otherwise known as RECs.[12] These RECs include: the Arab Maghreb Union (AMU);[13] the COMESA;[14] the Community of Sahel-Saharan states (CEN-SAD);[15] the East African Community

[9] Ibid.

[10] See art 3 of the Constitution of the African Union (9. 9. 1999). The Constitution was adopted at the thirty sixth ordinary session of the Assembly of Heads of States and Governments on 11 July 2000 at Lome, Togo. See Constitutive Act of the African Union (1999) http://www1.uneca.org/Portals/ngm/Documents/Conventions%20and%20Resolutions/constitution.pdf (date of use: 15 December 2015).

[11] See African Union 'History' http://www.au.int/en/about/history (date of use: 9 December 2015); and McNamee T; Mills G; and Pham J.P 'Morocco and the African Union: prospects for re-engagement and progress on the Western Sahara' (Discussion paper 1/2013) 1-27 http://www.thebrenthurstfoundation.org/Files/Brenthurst_Commissioned_Reports/Brenthurst-paper-201301-Morocco-and-the-AU.pdf (date of use 27 December 2015).

[12] For a general discussion of these RECs see: The Department of International Relations and Cooperation (RSA) 'Regional Economic Communities (RECs)' http://www.dfa.gov.za/au.nepad/recs.htm (date of use: 9 December 2015); United Nations Economic Commission for Africa (UNECA) 'History and background of Africa's regional integration efforts' https://www.uneca.org/oria/pages/history-africa's-regional-integration-efforts (date of use: 9 December 2015); also Vere A 'Legal and Regulatory frameworks for the knowledge economy: concept paper' E/ECA/CODIST/1/15 (29 March 2009) http://repository.uneca.org/bitstream/handle/10855/3452/Bib-27924.pdf?sequence=1 (date of use: 9 December 2015) for an overview on the current status of cyber laws in Africa; and Ndomo A 'Regional Economic Communities in Africa: A progress overview' (May 2009) http://www2.gtz.de/wbf/4tDx9kw63gma/RECS_Final_report.pdf 25-35 (date of use: 9 December 2015.

[13] AMU was established in 1989. It entered into a treaty to coordinate and harmonise and rationalise its policies and strategies for sustainable development in all sectors of human activity. See UNECA 'UMA Arab Maghreb Union: Treaty/Protocols' http://www.uneca.org/oria/pages/uma-arab-maghreb-union-0 (date of use: 9 December 2015).

[14] This REC is discussed in paras 5.2.3.1 and 5.3.3 below.

[15] CEN-SAD was established in 1998 as a framework for integration and complementarity which intends to work with the other regional economic communities and the AU to strengthen peace, security, and stability, and to achieve economic and social development. See UNECA CEN-

(EAC);[16] the Economic Community of Central African States (ECCAS);[17] the Economic Community of West African States (ECOWAS);[18] the Intergovernmental Authority for Development (IGAD);[19] and SADC.[20]

The four pillars regarded as constituting the basic tenets of regional integration are:[21] harmonisation of sectoral policies in infrastructure, natural resources, climate, food, and agriculture; macroeconomic policy convergence and financial and monetary integration; peace and security, stability and governance; and trade and market integration.

Not every treaty or protocol covers all sectors in the REC, but alignment with the four pillars is evident in the eight REC protocols and treaties.[22] While the integration is in

SAD 'Community of Sahel-Saharan states' http://www.uneca.org/oria/pages/cen-sad-community-sahel-saharan-states-0 (date of use: 9 December 2015).

[16] EAC was established in 1999 and came into operation in July 2000 when a treaty was entered into between three partner states – Kenya; Uganda and Tanzania – with the aim of widening and deepening cooperation among partner states in, among others, political, economic and social fields for their mutual benefit. See UNECA 'EAC Eastern African Communities' http://www.uneca.org/oria/pages/eac-east-african-community-0 (date of use: 9 December 2015).

[17] ECCAS was established on 18 October 1983 to form a wider economic community of Central African states. See UNECA 'ECCAS Economic Community of Central African States' http://www.uneca.org/oria/pages/eccas-economic-community-central-african-states-0 (date of use: 9 December 2015).

[18] ECOWAS was formed in 1975 mainly to promote cooperation and integration in the context of an economic union of West Africa in order to raise the living standards of its people and also maintain and increase economic stability. See UNECA 'History and background of Africa's regional integration efforts' http://www.uneca.org/oria/pages/ecowas-economic-community-west-african-states-0 (date of use: 9 December 2015).

[19] IGAD was established in 1996 in East Africa. IGAD superseded the Inter-governmental Authority on Drought and Development (IGADD) which was established in 1986. See UNECA 'History and background of Africa's regional integration efforts' http://www.uneca.org/oria/pages/history-bacground-africas-regional-integration-efforts (date of use: 9 December 2015); and African Union 'Intergovernmental Authority for Development (IGAD)' http://www.au.int/en/recs/igad (date of use: 9 December 2015).

[20] This REC is discussed in paras 5.2.3.2 and 5.3.4.2 below.

[21] See UNECA 'Regional integration tenets and pillars' http://www.uneca.org/oria/pages/regional-integration-tenets-and-pillars (date of use: 9 December 2015); Questia 'Four strategic pillars to guide the African Union: Commission's activities 2009-2012' https://www.questia.com/magazine/1G1-203770101/four-strategic-pillars-to-guide-the-african-union (date of use: 9 December 2015).

[22] Ibid. The main objectives of the RECs are: "to strengthen peace, security and stability and achieve economic and social development; to achieve sustainable growth and development of member states by promoting a more balanced and harmonious development of their production and marketing strategies; to promote, develop, transfer, and master technology; and to coordinate and harmonise international relations of member states and secure international understanding". See Ndomo A 'Regional Economic Communities in Africa: a progress overview' (May 2009) http://www2.gtz.de/wbf/4tDx9kw63gma/RECS_Final_report.pdf (date of use: 9 December 2015); and Dube M 'Traditional and emerging partners' role in African

place there remain certain challenges which include: multiple and overlapping membership which creates a complex web of competing commitments, and harmonisation and coordination among member states.[23] Below the backgrounds to two of the RECs – SADC and COMESA – and also the background of the ATU are examined. This is followed by a discussion of initiatives undertaken to combat spam in the AU with particular reference to SADC and COMESA.

5.2.3.1 COMESA

The COMESA came into being in December 1994 to replace its predecessor the Preferential Trade Area (PTA) which had existed since early 1981.[24] COMESA was established as an organisation of free independent sovereign states which agreed to cooperate in developing their natural and human resources for the good of all their people.[25] The main focus of COMESA is on the formation of a large economic and trading unit capable of overcoming some of the barriers faced by individual states.[26]

The treaty establishing COMESA was signed on 5 November 1993 in Kampala, Uganda, and was ratified a year later in Lilongwe, Malawi.[27] COMESA's objectives include: to achieve sustainable growth and development in member states by promoting a more balanced and harmonious development of their production and marketing strategies.[28] Currently COMESA has nineteen member states.[29]

Regional Economic Integration: Issues and recommendations' *SAIIA* Occasional Paper No 158 Economic Diplomacy Project (Oct 2013) http://dspace.africaportal.org/jspui/bitstream/123456789/1/saia_sop_158%20_dube_20131204 (date of use: 9 December 2015) for a background study of the REC's.

[23] Ibid.

[24] See COMESA 'About COMESA' http://about.comesa.int/index.php?option=com_content&view=Article&id=75&Itemid=106 (date of use: 9 December 2015). For the history of COMESA, see COMESA 'Looking back: Evolution of PTA/COMESA' http://about.comesa.int/index.php?option=com_content&view=article&id=95&Itemid=117 (date of use: 9 December 2015); and UNECA 'COMESA Common Market for Eastern and Southern Africa Protocols/Treaties' http://www.uneca.org/oria/pages/uma-arab-maghreb-union-0 (date of use: 9 December 2015).

[25] Ibid COMESA 'About COMESA'.

[26] Ibid.

[27] Ibid.

[28] See art 3 of the Common Market Treaty of the Common Market for Eastern and Southern Africa (1993) for a list of aims and objectives of COMESA.

[29] COMESA 'COMESA member states' http://about.comesa.int/index.php?option=comcontent&view =article&id=123&Itemid=121 (date of use: 9 December 2015).

5.2.3.2 SADC

The SADC is an organisation of member states in the southern region of Africa and was established on 17 August 1992.[30] SADC was preceded by the Southern African Development Coordination Conference (SADCC)[31] in 1980.[32] The SADC Treaty effectively launched a scheme for economic integration.[33] The SADC is a decentralised organisation with a small secretariat based in Gaborone, Botswana. South Africa became a member in 1994 after the abolition of apartheid.

The objectives of the SADC are among others:[34] (a) to promote self-sustaining development on the basis of collective self-reliance and the interdependence of member states; and (b) to strengthen and consolidate the long-standing historical, social, and cultural affinities and links among the people of the region. In order to achieve these objectives the SADC is mandated to promote the development and transfer of technology.[35] It is also tasked with coordinating and harmonising international relations of member states and securing international understanding, cooperation, and support.[36] Importantly, the SADC must mobilise the inflow of public and private resources into the region.[37]

5.2.3.3 ATU

[30] Currently SADC comprises of fifteen member states. Ten member states – Angola, Botswana, Lesotho, Malawi, Mozambique, Namibia, Swaziland, Tanzania, Zambia and Zimbabwe – signed a Declaration, Treaty and Protocol in 1993. See SADC 'Member states' http://www.sadc.int/member-states (date of use: 9 December 2015).

[31] SADCC was established on 1 April 1980 when the Lusaka Declaration was adopted by nine heads of states. South Africa was excluded because of its apartheid regime. For the background history of SADC see AU 'Southern African Development Community (SADC)' http://www.au.int/ en/recs/sadc (date of use: 9 December 2015); and Saurombe (2009) 21 *SA Merc LJ* 697-9.

[32] See UNECA 'SADC Southern African Development Community' http://www.uneca.org/oria/ pages/sadc-southern-african-development-community-0 (date of use: 9 December 2015).

[33] Declaration and Treaty of the Southern African Development Community (17 August 1992) 1-30 http://www.sadc.int/files/8613/5292/8378/ Declaration_Treaty-of-SADC.pdf (date of use: 9 December 2015). Hereafter referred to as 'the Declaration and Treaty of SADC'.

[34] Id art 5(1) for a list of these objectives.

[35] Id art 5(2).

[36] Ibid.

[37] Ibid.

The ATU was established in 1977 as a specialised agency of the OAU in the field of telecommunications.[38] The ATU adopted its current name in 1999 when it was transformed into a partnership between public and private stakeholders in the ICT sector.[39] In addition to providing a forum for stakeholders involved in ICTs, it also formulates effective policies and strategies aimed at improving access to information, infrastructure and services.[40] The ATU also represents the interests of its members at global decision-making conferences and promotes initiatives aimed at integrating regional markets, attracting investment into the ICT infrastructure, and building institutional and human capacity.[41]

The ATU's goals include enhancing Africa's contribution to global decision-making conferences and ensuring an equitable share of global resources.[42] The ATU currently has 44 member states and sixteen associate members (fixed and mobile telecom operators).[43]

Now that the backgrounds to the AU, certain of its RECs, and the ATU have been highlighted, the initiatives taken by these stakeholders to combat spam are reviewed.

5.3 Combating spam in the African region

5.3.1 Introduction

In the past decade the African region has been in the process of harmonising its ICT laws and developing laws where there are none.[44] These laws include: e-commerce

[38] For the history of the ATU see: ATU 'History' http://www.atu-uat.org/index.php/about-us/history (date of use: 9 December 2015).

[39] Ibid.

[40] Ibid.

[41] Ibid.

[42] See ATU 'Goals Strategies' http://www.atu-uat.org/index.php/about-us/core-activity-programmes/global-decision-making (date of use: 9 December 2015).

[43] ATU 'ATU member states as at 25th April 2013' http://www.atu-uat.org/index.php/members/member-states (date of use: 9 December 2015).

[44] See the following projects dealing with harmonisation: United Nations Conference on Trade and Development (UNCTAD) 'Harmonization of Cyberlaws and Regulation: The Experience of the East African Community (Reforming Cyberlaws Part 1)' UNCTAD/DTL/STICT/2012/4/Corr.1. http://unctad.org/en/PublicationsLibrary/dtlstict2012d4_en.pdf (date of use: 9 December 2015).

laws;[45] protection of privacy laws;[46] and, of late, cybercrime and cybersecurity laws or a combination of all three categories.[47] In this section, the documents and/or instruments developed in Africa to combat spam are examined. In Africa this issue is, in the main, addressed in multi-purpose legislation and/or general-purpose instruments, for example, Model Laws and/or Conventions.

5.3.2 African Union

5.3.2.1 Background

In 2009 at an extraordinary AU Conference, the AU Commission was requested to develop, jointly with the UNECA, a convention on cyber legislation based on the Continent's needs and adhering to the legal and regulatory requirements of electronic transactions, cybersecurity, and personal data protection.[48] In 2011 the AU released its "Draft Legal Framework on Cybersecurity in Africa".[49] This Draft Convention embodied the existing commitments of AU member states at sub-regional and international levels, to build the information society.[50] It also sought to define the objectives and broad orientation of the information society in Africa and to strengthen existing information and communication legislation in member states and regional communities.[51] The major challenge facing the Draft Convention was to achieve a level of technological security adequate to prevent and effectively control technological and informational risks.[52] The Draft Convention was adopted at the AU

[45] For a discussion on e-commerce in Africa see the following: Ndonga (2012) 5 *African Journal of Legal Studies* 243-68; 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* 550-76; Bwalya 'E-commerce penetration' 235-53; and Esselaar & Miller (2002) 2/1 *South African Journal of information and Communication* 1-12.

[46] See Greenleaf & Georges (2014) 132 *Privacy Laws and Business International Report* 19-21.

[47] See generally Uchenna JO 'Multilateral legal responses to cyber security in Africa: Any hope for effective international cooperation?' Paper presented at the 7th International Conference on Cyber Conflict (2015) https://ccdcoe.org/cycon/2015/proceedings/08_orji.pdf (date of use: 27 December 2015).

[48] See African Union 'Oliver Tambo Declaration' *Extra-Ordinary Conference of African Union Ministers in Charge of Communication and Information Technologies* Johannesburg, South Africa (2-5 November 2009); also African Union INFOSOC 'Cyber Security' http://pages.au/int/infosoc/cybersecurity (date of use: 9 December 2015).

[49] See African Union 'Draft African Union Convention on the Establishment of a Credible Legal Framework for Cybersecurity in Africa' http://au.int/en/cyberlegislation (date of use: 9 December 2015). Hereafter referred to as 'the Draft Convention'.

[50] Id 5.

[51] Ibid.

[52] Id 2-3.

Summit in June 2014 as the African Union Convention on Cyber Security and Personal Data Protection.[53]

5.3.2.2. African Union Convention on Cyber Security and Personal Data Protection

(a) Preamble to the Convention

The preamble to the African Union Convention on Cyber Security and Personal Data Protection[54] seeks to: harmonise African cyber legislation on e-commerce and cybercrime control.[55] It also aims to define the objectives and broad orientation of the information society in Africa and to strengthen existing legislation in member states and the RECs regarding ICTs.[56] The AU also seeks to establish a regulatory framework on cyber-security and personal data protection which takes into account the requirements of respect for the rights of citizens guaranteed under the fundamental texts of domestic law and protected by international human rights Conventions and Treaties, particularly the African Charter on Human and People's Rights.[57] The Convention seeks "to modernise instruments for the repression of cybercrime by formulating a policy for the adoption of new offences specific to ICTs, and aligning certain offences, sanctions, and criminal liability systems in force in member states".[58]

The Convention is divided into three parts: electronic transactions;[59] the personal data protection;[60] and the promotion of cybersecurity and combating of cybercrime.[61]

[53] See African Union (AU) Convention on Cyber Security and Personal Data Protection adopted by the 23rd Ordinary Session of the Assembly of the Union (27 June 2014, Malabo) 1-40 https://ccdcoe.org/sites/default/files/documents/AU-270614-CSConvention.pdf (date of use: 9 December 2015).

[54] Hereafter referred to as 'the AU Convention'.

[55] See AU Convention supra n 53 1-3.

[56] Ibid.

[57] Ibid. It also seeks to pursue the principles of the African Information Society Initiative and the African Regional Action Plan for the Knowledge Economy (ARAPKE).

[58] Ibid.

[59] This part is divided into three sections dealing with a variety of issues namely: s 1 electronic commerce especially art 4. Other articles include contractual liability of the provider of goods and services by electronic means (art 3); s 2 deals with contractual obligations in electronic form (which includes: art 5: electronic contracts; and art 6: writing in electronic form); and s 3 covers security of electronic transactions.

[60] This chapter includes issues such as: personal data protection (s 1); institutional framework for the protection of personal data (s 2); obligations relating to conditions governing personal data protection (s 3); and data subjects' rights (s 4).

Spam is dealt with specifically in Chapter I of the Convention which covers electronic transactions, and in particular section 1 which deals with electronic commerce. Only the electronic commerce section of the Convention will be discussed here.

(b) Combating spam under the AU Convention

Electronic commerce

The Convention defines electronic commerce as "the act of offering, buying, or providing goods and services via computer systems and telecommunication networks such as the Internet, or any other network using electronic, optical or similar media for distance information exchange".[62] It requires that certain information be provided by those persons involved in e-commerce activities to those who will be accessing goods and services.[63] Article 4 of the Convention contains provisions on advertising by electronic means.

Article 4: Advertising by electronic means

Article 4 of the AU Convention provides:

> 1. Without prejudice to Article 3[64] any advertising action irrespective of its form accessible through an online communication service, shall be clearly identified as such. It shall clearly identify the individual or corporate body on behalf of whom it is undertaken;
> 2. The conditions governing the possibility of promotional offers as well as conditions for participating in promotional competitions or games where such offers, competitions or games are electronically disseminated, shall be clearly spelt out and easily accessible;
> 3. State Parties of the African Union shall prohibit direct marketing through any kind of indirect communication using in any form the particulars of an individual who has not given prior consent to receiving the said direct marketing through such means;

[61] Chapter III covers promoting cyber security and combating cybercrime. The following sections are outlined: cybersecurity measures to be taken at national level (s 1); and criminal provisions (s II).

[62] See art 1 of the AU Convention. This definition is an improvement on the one in the Draft Convention which defined electronic commerce as "an activity by which a person offers or provides goods and services remotely or by electronic means". Contrast with art 1 s 1 of the Draft Convention supra n 49.

[63] This information includes: the name of the vendor and, in the case of a legal person, its corporate name; registration number; full address of the place of establishment; and e-mail addresses. For the scope and application of electronic commerce, see art 2 of the AU Convention.

[64] See art 3 of the AU Convention which deals with the contractual liability of the provider of goods and services by electronic means.

4. The provisions of Article 4.2 above notwithstanding direct marketing by electronic mail shall be permissible where:
   (a) The particulars of the addressee have been obtained directly from him/her;
   (b) The recipient has given consent to be contacted by the marketing partners;
   (c) The direct marketing concerns similar products or services provided by the same individual or corporate body.
5. State parties shall prohibit the transmission for the purposes of direct marketing of messages by means of any form of indirect electronic communication without indicating valid particulars to which the addressee may send a request to stop such communications without incurring charges other than those arising from the transmission of such a request.
6. State parties undertake to prohibit concealment of the identity of the person on whose behalf the advertisement accessed by an online communication service is issued.

(c) Commentary on the AU Convention

It has been noted that most African states are lagging behind when it comes to strengthening cyber security and fighting cybercrime, but that by adopting this Convention, Africa will have taken the first step toward aligning itself with international best practices.[65] Africa also understands that spam is a global phenomenon that can be combated only through the cooperation of all stakeholders. In what follows the Convention is discussed in general and the specific provisions governing advertising by electronic means.

General comments on the Convention

(i) Structure

The AU Convention is a multi-purpose document which covers the following three issues: electronic commerce; personal data protection; and cybercrime and cybersecurity. As outlined above, these three topics are addressed in three chapters each of which concentrates on issues relevant to the topic covered. The final structure of the Convention is a major improvement on earlier drafts. For example, in the 2012 Draft Convention the three parts each listed definitions, as opposed to the

[65] Tamarkin E ‘The AU’s cybercrime response: a positive start, but substantial challenges ahead’ Policy Brief 73 (January 2015) 1-8 https://www.issafrica.org/publications/policy-brief/the-aus-cybercrime-response-a-positive-start-but-substantial-challenges-ahead (date of use: 27 December 2015).

current Convention in which article 1 contains definitions applicable to the Convention as a whole.[66]

(ii) Benefits of the Convention

Some opine that the mere fact that the AU has adopted overarching policy on cybersecurity is already a significant step forward for the continent which has to date been viewed as a safe haven for cybercriminals.[67] Africa is noted by some as being home to four of the ten countries with the highest cybercrime rates in the world.[68] The AU Convention highlights the importance of adhering to national constitutional human rights law with particular emphasis on the African Charter on Human and People's Rights and this is to be welcomed,[69] as is the fact that the Convention outlines safeguards for citizens with regard to the processing of personal data.[70]

(iii) Criticism of the Convention

As noted above the current AU Convention was ratified in June 2014 after a delay occasioned by protest and criticism from certain stakeholder of provisions in the Draft Convention. Kenya drafted a petition to block its adoption listing, among other things, that "the Convention allowed African states to process personal and sensitive data without the owner's consent on the basis of state security and public interest".[71]

[66] See the Draft Convention supra n 49 in particular: Part 1 on electronic transactions, s 1 contained a list of definitions relating to that issue; Part II dealt with personal data protection, and s 1 had a list of definitions; and Part III dealt with promoting cybersecurity and combating cyber-crime.

[67] Roigas H 'Mixed feedback on the African Union Convention on Cyber security and Personal Data Protection' https://ccdcoe.org/mixed-feedback-african-union-convention-cyber-security-and-personal-data-protection.html (date of use: 9 December 2015); also Finnan D 'Africa: Lack of laws governing cybercrime making Africa a safe haven for Cybercriminals' http://allafrica.com/stories/201502161962.html (date of use: 27 December 2015); and Tamarkin supra n 65 1-8.

[68] Macharia J 'Africa needs a cybersecurity law but AU's proposal is flawed, advocates say' http://techpresident.com/news/wegov/24712/africa-union-cybersecurity-law-flawed (date of use: 27 December 2015); and Accessnow 'Emerging threats in cybersecurity and data protection legislation in African Union countries' https://www.accessnow.org/emerging-threats-in-cybersecurity-data-protection-in-african-union (date of use: 27 December 2015).

[69] Ibid Macharia.

[70] Ibid. See in particular, arts 13 of the AU Convention for the basic principles governing personal information.

[71] Githaiga G 'A Report of the online debate on African Union Convention on Cybersecurity (AUCC)' (December 2013) 1-23 http://www.iitpsa.org.za/wp-content/uploads/2014/02/REPORT-ON-OF-THE-ONLINE-DEBATE-ON-AFRICA-UNION-

This, it was felt, endangered the privacy of subjects and limited freedom of speech.[72] It also noted that rather than explicitly establishing a model legal framework which African countries could adopt, the Draft Convention merely created guidelines for African states when developing cybersecurity laws.[73] Many clauses in the AU Convention (as opposed to the Draft Convention) are said to provide for stringent control over and restriction on how developers may implement apps, many of which touch on electronic commerce and personal data collection and processing.[74] Internet sites and content developed outside of Africa – including popular social media sites – may elect not to offer their solutions in Africa as it may not make economic sense to comply with the stringent requirements in a region that barely contributes to their revenue.[75] The broad scope of the AU Convention has also been cited as a matter of concern.[76] Others have also raised serious concerns about the human rights implications, particularly those provisions that might support discrimination and expand government power.[77] The AU addressed these criticisms in May 2014 and finally adopted the Convention in June of that year.[78]

Provisions governing advertising by electronic means

CONVENTION-ON-CYBERSECURITY.pdf (date of use: 27 December 2015); Ugwu P 'Analyst picks holes in proposed AU Cybersecurity Convention' http://www.nigeriacommunicationsweek.com.ng/e-business/analyst-picks-holes-in-proposed-au-cybersecurity-convention (date of use: 27 December 2015); and Roigas supra n 67.

[72] Accessnow 'Africa moves towards a common cybersecurity legal framework' http://www.acessnow.org/blog/2014/06/02/africa-moves-toward-a-common-cyber-security-legal-framework (date of use: 9 December 2015) for other contentious provisions; and Van Zyl G 'Adoption of the "flawed" AU cybersecurity convention postponed' http://www.itwebafrica.com/ict-and-governance/523-africa/232273-adoption-of-flawed-au-cybersecurity-convention-postponed (date of use: 9 December 2015).

[73] See Uchenna supra n 47 128. Uchenna also notes that "the language of the Draft Convention does not intend these directives to create an explicit legal framework for the criminalisation of cybercrime or for cybersecurity, and that the adoption and ratification of the Draft Convention by African states will not suffice unless states individually enact cybersecurity laws that meet the guidelines in the Convention. It is also not guaranteed that the enactment of those laws will be uniform for the purpose of regional harmonisation as the draft does not explicitly establish a Model Law for countries to adopt".

[74] Mbuvi D 'African countries propose stringent rules governing ecommerce and data' http://www.cio.co.ke/news/main-stories/african-countries-propose-stringent-rules-governing-ecommerce-and-data (date of use: 27 December 2015).

[75] Ibid.

[76] Tamarkin supra n 65.

[77] Fidler M and Madzingira F 'The African Union Cybersecurity Convention: a missed human rights opportunity' http://blogs.cfr.org/cyber/2015/06/22/the-african-union-cybersecurity-convention-a-missed-human-rights-opportunity/ (date of use: 27 December 2015); Jackson T 'Can Africa fight cybercrime and preserve human rights' http://www.bbc.com/news/business-32079748 (date of use: 27 December 2015).

[78] Roigas supra n 67.

(i) Definitions

The Convention defines a number of terms, notably, direct marketing,[79] electronic communications;[80] indirect electronic communications,[81] electronic mail,[82] and consent of data subject.[83] However, there is no definition of unsolicited commercial communications or advertising, although it is clear from article 4 of the AU Convention that spam involves the solicitation or advertising of promotional items.[84] Interestingly, the term direct marketing includes solicitation carried out through message dispatch, irrespective of the message base or nature of the message.[85] This applies, in particular, to commercial, political, or charitable messages designed indirectly to promote goods and services or the image of a person selling goods or providing a service.[86] Political and charitable messages fall under the term "direct marketing" in so far as they too can promote goods and services.[87] The AU would, therefore, regard such messages as spam.

(ii) Mechanism for regulation

[79] Article 1 of the AU Convention defines "direct marketing" as "the dispatch of any message that seeks to directly or indirectly promote goods and services or the image of a person selling such goods or providing such services. It also refers to any solicitation carried out through message dispatch, regardless of the message base or nature, especially messages of commercial, political or charitable nature, designed to promote indirectly goods and services or the image of a person selling goods or providing the service".

[80] See art 1 of the AU Convention which defines the term "electronic communications" as "any transmission of signs, signals, written material, pictures, sounds or messages of whichever nature to the public or a sector of the public by electronic or magnetic means of communication".

[81] See art 1 of the AU Convention where the term "indirect electronic communication" is defined as "any text, voice, sound, or image message sent over an electronic communications network which is stored in the network or in the recipient's terminal equipment until it is collected by the recipient".

[82] See art 1 of the AU Convention which defines "electronic mail" as "any message in the form of text, voice, sound, or image sent by a public communication network, and stored in a server of the network or in a terminal facility belonging to the addressee until it is retrieved".

[83] Article 1 of the AU Convention defines the term "consent of data subject" as "any manifestation of express, unequivocal, free, specific and informed will by which the data subject or his/her legal, judicial or treaty representative accepts that his/her personal data be subjected to manual or electronic processing".

[84] See the following articles where these phrases are used: "advertising action" (art 4(1)); "promotional offers and promotional competitions" art 4(2)).

[85] See direct marketing definition in art 1 of the AU Convention.

[86] Ibid.

[87] Ibid.

As is clear from article 4, the Convention takes a restrictive approach to dealing with direct marketing and solicitation issues and adopts the opt-in mechanism.[88] Article 4 requires that a relationship be established before any marketing can be solicited, and that consent be given before that solicitation.[89] Even though consent is required, the AU Convention is silent on the form this consent should take.

(iii) Other requirements for sending electronic messages

What is encouraging about the AU Convention is that it gives rise to certain prohibitions that the ITU and the OECD have highlighted. These include the accurate labelling of advertisements before spam mail can be sent thus eliminating the problems surrounding the falsification of information or deliberately misleading the recipients of the messages.[90] This allows recipients either to take part in those promotional activities, or not to take part as the e-mail will be properly labelled. The issue of spoofing and disguising headers is also covered in the AU Convention,[91] as is the harvesting of addresses, albeit indirectly under the data protection provisions.[92]

The AU Convention further gives data subjects a right to be informed before their personal data can be disclosed for the first time to third parties or used on their behalf for purposes of marketing.[93] It further entitles the data subject to object, free of

[88] Phrases such as "shall prohibit direct marketing" (art 4(2)); and "shall prohibit the transmission for purposes of direct marketing" (art 4(5)) allude to that fact.

[89] Article 4(4) lists instances where direct marketing is permissible which includes: "whether the particulars of the addressee have been obtained directly from them; the recipient has given consent to be contacted by the marketing service; and that the direct marketing concerns similar products or services provided by the same individual or corporate body".

[90] See art 4(1) of the AU Convention which provides that "any advertising action irrespective of its form accessible through an online communication service shall be clearly identified as such". Also art 4(2) of the AU Convention which provides that "promotional competitions disseminated electronically shall be clearly spelt out and easily accessible".

[91] Article 4(6) (1) of the AU Convention provides that "the individual or corporate body on behalf of whom the advertising is undertaken shall be clearly identified". Also art 4(6) of the AU Convention which "prohibits concealment of the identity of the person on whose behalf the advertisement accessed by an online communication service is issued".

[92] See in particular, art 13 of the AU Convention which addresses the basic conditions for processing the personal information of data subjects. These principles include: the principle of consent; the principle of lawfulness and fairness of personal data processing; the principle of purpose, relevance and storage of processed personal data; the principle of accuracy of personal data; the principle of transparency of personal data processing; and the principle of confidentiality and security of personal data processing.

[93] See art 18 of the AU Convention.

charge, to such disclosures.[94] All these provisions could go a long way to minimising the issue of harvesting and/or the sale of e-mail address lists for marketing purposes. The AU Convention is, however, silent when it comes to uses such as dictionary attacks and the issue of software used to generate e-mail addresses for purposes of spam. Be that as it may, the AU Convention has at least put some basic elements in place to regulate the sending of commercial or promotional communications. And, since the AU itself welcomes amendments to the provisions in the Convention, problematic aspects can receive the necessary attention at a later date as part of the effort to ensure that proper measures are put in place.[95] In the previous chapter it was noted that spam is now commonly used for phishing and other malicious acts. The Convention's cyber security provisions include a call for international cooperation to address this threat.[96] Although those provisions do not deal specifically with the issue of spam, they can nonetheless be used to enforce cooperation in the fight against spam at the global level.

(iv) Penalties

State parties shall take necessary legislative measures to ensure that offences provided under the AU Convention are not only punishable by effective, proportionate, criminal penalties,[97] but that they are also punishable by appropriate penalties under member states' national legislation.[98] State parties are required to take the necessary legislative measures to ensure that those held liable pursuant to the terms of the AU Convention, are punishable by effective and proportionate sanctions.[99]

These criminal sanctions include state parties taking the measures necessary to ensure that in the case of a conviction for an offence committed through a digital

[94] Ibid.

[95] See art 37(1) of the AU Convention. The amendments are to be submitted to the Chairperson of the Commission of the AU who shall transmit them to state parties within 30 days of receipt (art 37(2)). Upon recommendation from the Executive Council of the Union, the proposals will be considered at one of the sessions (art 37(3)), and the amendments shall be adopted in accordance with its rules of procedure (art 37(4)).

[96] See art 28 of the AU Convention.

[97] Id art 31(1)(a).

[98] Id art 31(1)(b).

[99] Id art 31(1)(c).

communication medium, a competent court may impose sanctions.[100] For example, the judge may order the mandatory dissemination, at the expense of the convicted person, of an extract from his or her judgment using the same medium used for the original message and in accordance with the requirements prescribed by the law in the member state concerned.[101] A breach of the confidentiality of data stored in a computer system is punishable by the same penalties as those applicable to breaches of professional secrecy.[102]

Measures to be taken at AU level

The Convention further includes measures to be taken at AU level by requiring the chairperson of the Commission to report to the Assembly on the establishment and monitoring of the operational mechanism.[103] These include encouraging AU members to adopt and implement measures to strengthen cybersecurity in electronic services and to combat cybercrime and human rights violations in cyberspace.[104] It is further required to advise African governments on how to promote cybersecurity and combat the scourge of cybercrime and human rights violations in cyberspace at national level, and to gather information and carry out analyses of the criminal behaviour of information network users and computer systems operating in Africa.[105] This information must be transmitted to competent national authorities. It must also formulate and promote the adoption of harmonised codes of conduct for use by public officials in the area of cyber security, and carry out any other tasks relating to cybercrime and breaches of the rights of individuals in cyberspace as may be assigned to it by the policy organs of the AU.[106]

Signature and ratification

[100] Id art 31(2)(a-c).
[101] Ibid.
[102] Ibid.
[103] Id art 32.
[104] Ibid.
[105] Ibid.
[106] Ibid.

The Convention is open to all AU state parties[107] for signature, ratification, or accession in conformity with their respective constitutional procedures.[108] It remains to be seen which state parties will ratify the Convention and whether it will act as a protective measure against cybercrime in Africa including combating spam.[109] As of September 2016 no member state had yet ratified the Convention. Some member states are apparently considering Bills aimed at aligning their laws with the Convention.[110] Be that as it may, state parties who do not have laws in place to address the issue, would be wise to become party to the Convention and also draw from those state parties who have laws in place which appear to be providing greater protection and safeguards for their nationals.

In the discussion below, the stance taken to combat spam by the two RECs listed above, followed by the role of the ATU is highlighted.

5.3.3 COMESA Model Law on Electronic Transactions and its Guide to Enactment

5.3.3.1 Background

The COMESA Model Law on Electronic Transactions[111] has been following a programme on e-legislation aimed at assisting its member states to develop appropriate legislation to support e-commerce.[112] A study to develop e-legislation guidelines for the COMESA region was undertaken followed by two workshops on e-legislation in general and on e-commerce laws in particular.[113] The Model Law is drafted on the basis of United Nations Convention on the Use of Electronic

[107] Article 1 of the AU Convention defines the term "state party" or state parties as "member state(s) which has or have ratified or acceded to the present Convention".

[108] Id art 35.

[109] In terms of art 36 of the AU Convention, the Convention shall enter into force 30 days after the date of the receipt by the Chairperson of the Commission of the AU.

[110] Countries with proposed Bills on cybercrimes; cyber-security and data protection laws are: Botswana; Kenya; Madagascar; Mauritania; Morocco; Tanzania; Tunisia; and Uganda. See Finnan supra n 67.

[111] See COMESA Model Law on Electronic Transactions and Guide to Enactment (2010) 115, hereafter the 'COMESA Model Law'. It is also recommended that the Model Law be called Electronic Transactions Act rather than the Electronic Commerce Act as the former is said to provide a wider description than the latter. This is more in keeping with the nature and scope of the Model Law.

[112] See Executive Summary of the COMESA Model Law 1.

[113] Ibid.

Communications in International Contracts,[114] the United Nations Commission on International Trade Law Model Law on Electronic Commerce,[115] and the United Nations Commission on International Trade Law Model Law on Electronic Signatures.[116] The provisions of the COMESA Model Law apply to international transactions only – domestic transactions, therefore, do not fall within its ambit.[117] The COMESA Model Law is divided into five parts namely: general issues;[118] application of legal requirements to data messages;[119] communication of data messages;[120] consumer protection;[121] and online dispute resolution.[122] The issue of unsolicited commercial communications is dealt with under consumer protection provisions in Chapter IV of the Model Law.

5.3.3.2 Consumer protection

The COMESA Model Law makes provision for certain core information to be provided to consumers[123] and ensures for consumers the right to withdraw from a transaction if these requirements have not been met.[124] A "consumer" is defined as "any natural person who enters or intends entering into an electronic transaction with a supplier as the end user of the goods and services offered by that supplier".[125] The issue of unsolicited goods, services, or communications (spam) is dealt with under article 25 of the COMESA Model Law to be discussed below.

[114] Hereafter 'UNECIC'. See id 4.

[115] See United Nations Commission on International Trade Law Model Law on Electronic Commerce with Guide to Enactment (1996). Hereafter 'UNCITRAL'.

[116] See UNCITRAL Model Law on Electronic Signatures with Guide to Enactment (2001).

[117] See Executive Summary of the COMESA Model Law 2.

[118] See Chapter 1 of the COMESA Model Law. This chapter covers the following issues: sphere of application (art 1); definitions (art 2); interpretation (art 3); variation of agreement (art 4); and location of parties (art 5).

[119] Id Chapter II which covers the following: legal recognition of data message (art 6); writing (art 7); signatures (art 8); original form (art 9); admissibility and evidentiary weight of data messages (art 10); and retention of data messages (art 11).

[120] Id Chapter III which covers the following articles: formation and validity of contracts (art 12); and time and place of dispatch and receipt of data messages (art 19). For other provisions see arts 12-21.

[121] Id Chapter IV which covers among others: scope of application (art 22); information to be provided (art 23); and cooling off provisions (art 24) et cetera.

[122] Id Chapter V which covers issues such as conciliation before the court of justice of the Common Market (art 30).

[123] This information includes: the full name and legal status of the vendor; physical address and telephone number; e-mail and web site address; membership of any self-regulatory or accreditation bodies to which the supplier belongs (id art 23(1) for an exhaustive list of the information to be provided to consumers).

[124] See in particular art 23(2) - (4) of the Model Law.

[125] See art 2 of the COMESA Model Law.

5.3.3.3 Combating spam under the COMESA Model Law

Spam provisions under the COMESA Model Law are dealt with under Article 25. The title of the article is: Unsolicited goods, services, or communications

(a) Article 25: Unsolicited goods, services, or communications

Article 25 provides as follows:

> (1) That any person sending unsolicited communications to a consumer must provide the consumer with
> (a) the option to cancel such subscription to the senders mailing list; and also
> (b) identifying particulars of the source from which the sender obtained consumers personal information.
> (2) No agreement is concluded where the consumer has failed to respond to an unsolicited communication(s).
> (3) Any person who fails to comply with or contravenes subsection (1) is guilty of an offence and liable on conviction to a maximum fine of [currency and amount].
> (4) Any person who sends unsolicited commercial communications to a person, who has advised the sender that such communications are unwelcome, is guilty of an offence and liable, on conviction, to a maximum fine of [currency and amount].

(b) Commentary on the COMESA Model Law

The COMESA Model Law is accompanied by a "Guide to Enactment"[126] which comments on the provisions of the Model Law. The Guide provides a detailed explanation of how each article is intended to function in practice.[127] The Guide also serves as an aid to the interpretation of the Model Law once it has been enacted by member states.[128] Using the Guide for purposes of interpretation will also enhance the harmonising effect of the Model Law within the region.[129]

The commentary on article 25 in the Guide notes the following:[130]

> This article places an obligation on the sender of spam to provide consumers with an opt-out mechanism. It also gives the consumer a right to obtain information on where the person obtained their personal particulars. Non-compliance with this provisions is liable the payment of a fine or conviction.[131] Unlike other provisions where civil remedies were regarded as sufficient to protect the interests of consumers, in this instance, civil remedies were regarded as

[126] Hereafter 'the Guide'.

[127] See Executive Summary of COMESA Model Law 7.

[128] Ibid.

[129] Ibid.

[130] See the Guide 106.

[131] The COMESA Model Law has left it to state parties to indicate the amount of a fine for contravening the provisions of this article.

> ineffective in themselves to counter the problem of spam. Article 25 paragraph (2) is aimed at providing legal certainty and protection to consumers against another unconscionable selling technique, namely sending communications[132] purporting to be an offer which will be regarded as being accepted if a consumer should fail to respond to it. This is similar to the technique where unsolicited goods are sent followed by an invoice if the consumer does not return the goods within a specific time. This provision simply states that consumers will incur no obligations by failing to respond to unsolicited electronic communications from suppliers. Their silence is treated in law as a rejection in law rather than as an acceptance.

Consumers may also lodge a complaint with the relevant government department or Consumer Protection Organisation in respect of any non-compliance with the provisions of this Chapter by a supplier.[133]

(c) Shortcomings in the Model Law

The COMESA's Model Law deals with the issue of spam in a minimalist approach, offering only a basic description of provisions on how to regulate spam. It is important to note here that the provisions of the COMESA Model Law are identical to those in section 45 of the South African ECT Act of 2002.[134]

Lack of definitions

The COMESA Model Law describes spam as "unsolicited commercial communications",[135] "unsolicited communications",[136] and "unsolicited goods, services or communications".[137] However, it fails to define what these terms mean, although it is clear from the provisions that spam involves the content of the message – namely, its "commercial aspect" – rather than the "volume". There must be a sale or offer of goods and services before a communication can be classified as

[132] Article 2 of the COMESA Model Law defines the term "communications" as "any statement, declaration, demand, notice or request, including an offer and 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. Electronic communication, on the other hand, means communication by means of data messages".

[133] See art 29 of the COMESA Model Law. According to the commentary effectiveness of the remedy provided in this article will depend on the powers to which such complaints will be directed. It is not the only remedy but provides a further remedy to strengthen consumer rights. It also raises consumer awareness of other possible avenues through which to address their grievances. See the Guide 107.

[134] Section 45 of the ECT Act is dealt with in Chapter 8 par 8.2.5.1 below.

[135] See art 25(1) and (4) of the COMESA Model Law.

[136] Id art 25(2).

[137] See title of art 25 of the COMESA Model Law.

spam. In these terms, non-commercial e-mails – chain letters, urban legends, and the like – would not qualify as spam.

The COMESA Model Law, however, defines certain terms including "communications",[138] "consumer",[139] and "electronic communications".[140] However, certain concepts that are important in clarifying the issue of spam are not defined – for example, terms such as "electronic transactions",[141] "electronic commerce", and "personal information".[142]

Regulation rather than prohibition of spam

The COMESA Model Law follows the opt-out mechanism which regulates spam but does not prohibit it. Although the COMESA Model Law places an obligation on the sender to provide the consumer with an opt-out facility, it does not provide for the ways in which this mechanism is to be administered, so defeating the whole purpose of allowing the consumer to opt-out. As noted in the previous chapter, certain requirements must be met if this facility is to be administered successfully, and the COMESA Model Law fails to provide this information.[143] There is, therefore, no deterrent which would persuade the sender to stop sending further spam emails.

Other basic requirements governing the sending of e-mail that could assist in this regard are not spelt out. Notable here are e-mail harvesting, labelling requirements, and disguised headers. Without these requirements, consumers are unable to request particulars of how and where the spammer came by their personal information.

[138] Article 2 of the COMESA Model Law defines the term "communication" as "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".

[139] See para 5.3.3.2 above for the definition of consumer.

[140] Article 2 of the COMESA Model Law defines the term "electronic communications" as "a communication by means of data message". A "data message", in turn, is defined as "information generated, sent, received, or stored by electronic, optical or similar means including but not limited to electronic data interchange (EDI), e-mail; voice, where the voice is used in automated transactions; and a stored record". See art 2 of the COMESA Model Law.

[141] See the title of the COMESA Model Law.

[142] This term is used in art 25(1)(b) of the COMESA Model Law.

[143] See para 4.3.4.2 (c) (ii) in Chapter 4 above for the use of the opt-out facility.

According to the COMESA Model Law, the advantage of this instrument is that it is able to achieve a high level of harmonisation without the restrictions of a Convention.[144] As a result, member states are able to tailor the Model Law to national requirements and to take account of the differences and needs of domestic law.[145] The Model Law also allows for amendments to the national legislation of member states aimed at strengthening regulation.[146] In 2011 a decision was taken that state parties should adopt the Model Law.[147] Like the AU Convention above, it is not clear how many COMESA member states have signed or ratified the Model Law. Below is a discussion on the SADC Model Law.

5.3.4 SADC

5.3.4.1 Harmonisation of ICT Policies in sub-Saharan Africa

The Harmonisation of ICT Policies in Sub-Saharan Africa[148] is a project initiated as a result of a request from Economic Integration Organisations in Africa, as well as regional regulator associations, to the ITU and the European Commission for assistance in harmonising ICT policies and legislation in sub-Saharan Africa.[149] The project for harmonisation of ICT laws started in 2008 and culminated in the Southern region with the Electronic Transactions and Electronic Commerce Southern African Development Community (SADC) Model Law.[150] Consultants worked on the draft document which was later reviewed, discussed, and validated by broad consensus

[144] See Executive Summary of COMESA Model Law 4.

[145] Ibid.

[146] Ibid.

[147] The decision was made by the Council that the Electronic Transaction Model Bill be adopted. See art 38(a) *Official Gazette of the Common Market for Eastern and Southern Africa* 16 (15 October 2011).

[148] Hereafter 'HIPSSA'. HIPSSA is part of a global ITU-EC-ACP project being implemented through three sub-projects customised to the specific needs of each region: Sub-Saharan Africa (HIPSSA); the Caribbean (HIPCAR); and the Pacific Island Countries (ICB4PAC). See ITU 'HIPSSA project: Support for harmonization of the ICT policies in Sub-Saharan Africa' http://www.itu.int/en/ITU-D/Projects/ITU-EC-ACP/HIPSSA/Pages/default.aspx (date of use: 20 March 2017).

[149] Ibid. The project was divided into four sub-regional programs taking into account sensitive issues such as geographical, political, and cultural diversity in the region, and also to avoid potential competition between regional organisations. These sub-regions are East Africa, Central Africa, Southern Africa, and West Africa. The main aim of this project is to develop a strong, integrated and viable communications sector on the Continent.

[150] See the Southern African Development Community (SADC) Model Law on Electronic Transactions and Electronic Commerce (2013) iii. Hereafter 'the SADC Model Law'.

among participants at a workshop held in Gaborone, Botswana, in 2012.[151] One of the broad objectives of the HIPSSA is: to establish harmonised policy and legal and regulatory frameworks at the regional and continental levels; to create an enabling environment that will attract investment and foster the sustainable development of competitive African Telecommunication/ICT regional markets and infrastructures; and increase access to the related services for its people.[152]

This SADC Model Law was adopted by the SADC Ministers responsible for telecommunications, postal services, and ICT in their regions, at a meeting in Mauritius during 2012.[153] In addition to this Model Law, the Computer Crime and Cybercrime Model Law[154] was published in 2013. This Model Law also contains provisions relevant to spam. Although a discussion of the Model Law on Computer Crime and Cybercrime falls outside of the scope of this thesis, reference will be made to the relevant spam provisions in the discussion below.

5.3.4.2 SADC Model Law

(a) Background

According to the SADC Model Law the advent of the use of electronic communications for commercial transactions has posed unexpected and complex legal problems not only for SADC countries, but also for countries worldwide.[155] The SADC Model Law provides a tool that member states can use to create a more secure legal environment for electronic transactions and electronic commerce.[156] It also seeks to "enhance regional integration and has adopted the best practices and collective efforts of member states to address the legal aspects of e-transactions and

[151] Ibid.

[152] ITU HIPSSA Project 'Support for harmonization of the ICT policies in Sub-Saharan Africa' http://www.itu.int/en/ITU-D/Projects/ITU-EC-ACP/HIPSSA/Pages/default.aspx (date of use 30 November 2015).

[153] See SADC Model Law par iii.

[154] The Southern African Development Community Model Law on Computer Crime and Cybercrime *Harmonization of ICT Policies in Sub-Saharan African* (2013). This Model Law is aimed at the criminalisation and investigation of computer and network-related crime (Part 1 art 2 of the Model law).

[155] See Preamble to the SADC Model Law 1.

[156] Ibid.

e-commerce".[157] The SADC Model Law is divided into five parts: (a) general enabling provisions;[158] (b) electronic transactions;[159] (c) electronic commerce;[160] (d) consumer protection;[161] and (e) service providers.[162] Of importance for present purposes are the consumer protection provisions, and especially the issue of online marketing.

(b) Consumer protection

The issue of consumer protection under the SADC Model Law is dealt with in Part IV where Chapter 8 dealing with the protection of online consumers is located.[163] This chapter creates obligations for suppliers in that they are required to make specific information available to consumers.[164] Chapter 9 deals expressly with the issue of online marketing, while section 30 covers the issue of unsolicited commercial communications.

(c) Combating spam under the SADC Model Law

Spam provisions under the SADC Model Law are contained in section 30. The title of that section is unsolicited commercial communications. Section 30 provides:

> (1) Marketing by means of electronic communication shall provide the addressee with:

[157] Ibid.

[158] See Part I of the SADC Model Law dealing with: Chapter 1: definitions and interpretation (ss 1-3); Chapter 2: the legal recognition of electronic communications (ss 4-5); and Chapter 3: the legal effect of electronic communications (ss 6-9).

[159] See Part II of the SADC Model Law which encompasses: Chapter 4: the legal recognition of electronic transactions (ss 10-11); and Chapter 5: time and place of dispatch and receipt of electronic communications (ss 12-16).

[160] See Part III of the SADC Model Law which covers the following: chapter 6 attribution (sections 17-18); chapter 7 admissibility and evidentiary weight of electronic communications (sections 19-24).

[161] Id Part IV.

[162] See Part V of the SADC Model Law which deals with the following: Chapter 10: online safe harbours (ss 31-34); and Chapter 11: requirements (ss 35-37).

[163] Section 1 of the SADC Model Law defines the term "consumer" as "a natural person and or a non-profit organisation that purchases goods and services for the direct satisfaction of individual needs or wants, or the collective needs of members of a community; or a natural person who enters or intends entering into an electronic transaction with a supplier as the end user of goods or services offered by the supplier".

[164] This information includes the full contract details of senders; their place of business; and full price of the goods and services rendered. The supplier should also provide the consumer with the opportunity to review his or her transactions, correct mistakes, and withdraw from transactions, as well as a cooling off period. See ss 25(1) and (2) and 27 of the SADC Model Law.

(a) The originators identity and contact details including its place of business, e-mail addresses and telefax numbers;
(b) A valid and operational opt-out facility from receiving similar communications in the future; and
(c) The identifying particulars of the source from which the originator obtained the addressees personal information.

(2) Unsolicited commercial communications may only be sent to addressees where the opt-in requirement is met.

(3) The opt-in requirement will be deemed to have been met where:
(a) The addressee's e-mail address and other personal information was collected by the originator of the message in the course of a sale or negotiations for a sale;
(b) The originator only sends promotional messages relating to its "similar products and services" to the addressee;
(c) When personal information and address was collected by the originator, the originator offered the addressee the opportunity to opt-out (free of charge for the cost of transmission) and the addressee declined to opt-out; and
(d) The opportunity to opt-out is provided by the originator to the addressee with every subsequent message.

(4) No contract is formed where an addressee does not respond to an unsolicited commercial communication.

(5) An originator who fails to provide the recipient with an operational opt-out faculty referred to in subsections 1b and 3d is guilty of an offence and liable, on conviction, to the penalties prescribed in subsection 8.

(6) Any originator who persists in sending unsolicited commercial communications to an addressee who has opted out from receiving any further electronic communications from the originator through the originator's opt-out facility, is guilty of an offence and liable, on conviction, to the penalties prescribed in subsection 8;

(7) Any party whose goods or services are advertised in contravention of this section is guilty of an offence and liable, on conviction, to the penalties prescribed in subsection 8.

(8) A person convicted of an offence referred to in this section is liable on conviction to a fine or imprisonment for a period not exceeding five years.

(d) Commentary on the SADC Model Law(s)

The SADC Model Law is expressed in a technologically neutral manner so that it can be applied to existing technologies as well as those yet to be developed.[165] It also contains comprehensive anti-spam provisions. These provisions include, but are not limited to, the following:

Definitions

The SADC Model Law addresses the scope of application of key concepts and has proposed neutral definitions.[166] Provision is made for the following definitions:

[165] See Preamble to the SADC Model Law.
[166] See SADC Model Law 1.

"addressee";[167] "data message";[168] "electronic communications";[169] "electronic transactions";[170] "intermediary";[171] "originator";[172] and "place of business".[173] Some terms which could improve the reach of the SADC Model Law are, however, not defined. Notable among these are "marketing";[174] "e-mail";[175] "unsolicited commercial communications";[176] and "personal information".[177] However, it is clear from the term "unsolicited commercial communications" that the SADC Model Law regulates spam only in relation to its content and that any other malicious e-mails that do not have a commercial aspect, will not fall under this definition. This is consistent with the discussion above.

Mechanism for regulating spam

The SADC Model Law advocates for strict measures to regulate spam. It advocates the sending of unsolicited communications only once an opt-in requirement has been satisfied.[178] It also sets out requirements to be met where an opt-in requirement is needed which covers the fact that the recipient's e-mail address or personal information be collected by the originator.[179]

[167] The term "addressee of an electronic communication" means "any party who is intended by the originator to receive the electronic communications, but does not include a party acting as an intermediary in respect of that electronic communication". See s 1 of the SADC Model Law.

[168] Id s 1 which defines a "data message" as "information generated, sent, received, or stored by electronic, magnetic, optical or similar means, including but not limited to electronic data interchange (EDI), electronic mail, mobile communications (such as SMS messages) and audio or video recordings".

[169] The term "electronic communications" is defined as: "communication made by means of a data message". Ibid.

[170] An "electronic transaction" means "a transaction, action, or set of actions, of either a commercial or non-commercial nature, and includes the provision of information and or e-government services". Ibid.

[171] The term "intermediary with respect to a particular electronic communication", means "a person who on behalf of another person sends, receives, or stores that electronic communication or provides other services with respect to it". Ibid.

[172] The term "originator of an electronic communication" is defined as "a person or party by whom or on whose behalf the electronic communication purports to have been sent or generated prior to storage if any". This term does not include a person or party acting as an intermediary with respect to that communication. Ibid.

[173] The term "place of business" is defined as "any place where the party maintains a non-transitory establishment to pursue an economic activity other than the temporary provision of goods and services out of a specific location". Ibid.

[174] As used in s 30(1) of the SADC Model Law.

[175] As used in s 30(3)(a) of the SADC Model Law.

[176] As referred to in s 30(2), (4) and (6) of the SADC Model Law.

[177] Id s 30(1) (c), and (3) (a)(c).

[178] Id s 30(2).

[179] Ibid.

In this case the originator must provide the addressee with an option to opt-out from receiving similar communications in the future.[180] That opt-out facility must be valid and operational, and failure to provide this will render the originator guilty of an offence and liable on conviction to a fine or imprisonment not exceeding five years.[181]

Requirements for the sending of e-mail

Section 30(7) of the SADC Model Law also imposes liability on senders for advertising in contravention of these provisions. The SADC Model Law also requires that the originator provide the addressee with its identity and contact details which include: e-mail addresses and telefax to mention but a few.[182] Also required is that the recipient be provided with the identifying particulars of where the originator obtained the addressee's personal information.[183] The SADC Model Law does not address the following aggravated issues: address harvesting; the sale of e-mail address lists for marketing purposes; dictionary attacks; and the use of software to extract e-mail addresses from public sites.

The move towards a Model Law in the SADC region is a starting point in ensuring that member states in the region are prepared for the current electronic age. The SADC Model Law holds anyone liable (on conviction to either a fine or imprisonment not exceeding five years), who persists in sending communications after they have been instructed to stop.[184] It remains to be seen how the SADC member states will fare in adopting this Model Law in their national laws.[185]

SADC Model Law on Computer Crime and Cybercrime

[180] Id s 30(1) (b) and 3(d).

[181] Id s 30(1) (b), (5) and (6).

[182] Id s 30(1) (a). This will be helpful in cases where the addressees would like some information furnished regarding the source from which the originator or sender obtained their personal information.

[183] Id s 30(1) (c).

[184] Id s 30(6) and (8).

[185] It is unclear how many members have ratified this Model.

Other spam related provisions are located in article 19 of the SADC Model Law on Computer Crime and Cybercrime. This article prohibits the following unlawful acts committed by a person intentionally and without lawful cause or justification:[186] initiating the transmission of multiple e-mail messages[187] from or through such computer system;[188] the use of a protected computer system[189] to relay or re-transmit multiple e-mail messages with the intent to deceive or mislead users; or any e-mail or ISP[190] as the origin of such messages.[191] This article includes provisions on materially falsified header information in multiple e-mail messages and the intention of initiating the transmission of such messages.[192] The above activities are punishable on conviction, by imprisonment for a specified period or a fine not exceeding a specified amount, or both.[193] Countries may restrict the criminalisation with regard to the transmission of multiple electronic messages within a customer or business relationship.[194] Note should be taken here that these provisions has to do with the technological aspects of spam.

Below an outline of the ATU's position on spam is highlighted.

5.3.5 ATU

5.3.5.1 Cooperation between ATU and other stakeholders

As pointed out in Chapter 4, a meeting on countering and combating spam was held in July 2013, at which a partnership between the AU, the ATU, the ITU, and the ISOC was mooted.[195] The following action was identified as appropriate for

[186] See art 19(1) of the SADC Model on Computer crime and Cybercrime.

[187] Part 1 art 3(17) of the of the SADC Model on Computer Crime and Cybercrime defines the term "initiating the transmission of multiple e-mail messages" as "a mail message including e-mail and instant messaging sent to more than thousand recipients".

[188] Id art 19(1) (a).

[189] The term "computer system" or "information system" as "a device or a group of inter-connected or related devices, one or more of which, pursuant to a program, performs automatic processing of data or any other function". Id Part 1 art 3(5).

[190] The term "Internet service provider (ISP" is defined as "a natural or legal person that provides to users' services mentioned in arts 28-32 of the Model law". Id Part 1 art 3(21).

[191] Id art 19(1)(b).

[192] Id art 19(1)(c).

[193] Id art 19(1)(c).

[194] Iid art 19(2).

[195] ITU 'Workshop on countering and combating spam' (Durban South Africa 8 July 2013) http://www.itu.int/en/ITU-T/Workshops-and-Seminars/spam/201307/Pages/default.aspx (date of use: 30 November 2015).

partnerships and or agreements between the stakeholders, namely, to develop a Model Law governing spam (including SMS spam) based on existing laws that have proven effective.[196] This would include cybercrime laws, the ITU's work, the SADC Model Law on Computer and Cybercrime, and the AU Convention.[197] These were to be developed jointly by the AU and the UNECA. Inherent is the development of a model program for cooperation between governments and industry in national actions to combat spam – for example, agency cooperation to detect and take down botnets should also be taken into account.[198] This model program would be disseminated through workshops and other means with the aim of developing a program to assist African ISPs to implement effective anti-spam tools.[199] The development of information for users on how to protect themselves against spam, and also to identify suspicious messages and deal with them safely, was also included.[200]

In September of 2013 a seminar for policy makers on combating spam was also organised in Nairobi, Kenya.[201] This seminar offered government representatives, policy makers, and developing-country participants an opportunity to engage with technical experts, industry associations, and government agencies working to reduce the impact of spam.[202] The seminar provided an opportunity for open discussion on what tools to use, government requirements, and best practices for network management associated with combating the proliferation of spam, malware, botnets, and phishing based upon experiences and approaches currently in use.[203]

The meeting aimed to adopt actionable outcomes to provide meaningful technical and policy information on best practices, and also to meet the ATU spam action items identified at the July seminar in Durban, South Africa.[204] It further aimed to

[196] Ibid.

[197] See the AU Convention para 5.3.2 above.

[198] Ibid.

[199] ITU 'Workshop on countering and combating spam' supra n 194.

[200] Ibid.

[201] See Internet Society 'Program for joint ATU and the Internet Society seminar on combating spam' (9 September 2013 Nairobi Kenya) 1-2 http://www.internetsociety.org/sites/default/files/ATU%20Spam%20Agenda%20and%20Speakers.pdf (date of use: 9 December 2015).

[202] Ibid.

[203] Ibid.

[204] Ibid.

establish a multi-stakeholders process by which to bring Internet technical expertise, industry associations, and policy makers together to create a sustainable model for engagement and problem solving in combating spam in all its forms both within Africa and as part of the global community.[205] Now that the Model Laws and other initiatives in this region have been outlined, a contextualisation of the instruments follows below.

5.4 Contexualisation of the African Region's Model Laws and Conventions

The recent instruments for combating spam in Africa are an indication of the continent taking part in the knowledge economy by aligning itself with international best practices. What has emerged from the first-step on the road to harmonisation is that while there are areas in which harmonisation has been achieved, differences remain. It is noted that the instruments are either multi-purpose (for example, the AU Convention), or specific (the COMESA and SADC Model Laws).

5.4.1 Uniformity among instruments: definitions

The issue of spam is dealt with under consumer protection provisions in the COMESA and SADC Model Laws, whereas in terms of the AU Convention, spam is covered under its electronic commerce provisions. Both the COMESA and SADC Model Laws refer to spam as unsolicited commercial communications, while under the AU Convention spam is approached in relation to direct marketing and solicitation. In all three instruments the term "unsolicited commercial communications" or "spam" is undefined. What is, however, clear from those terms is that the classification of spam is based on the content of the message rather than its' "size". Consequently, any unsolicited communication sent to a receiver which has as its content the sale of goods and or services will be regarded as spam. Even where the AU Convention includes political and charitable messages in its definition of direct marketing, the content of such messages must still meet the requirement of the advertising of goods and services. With this mind, any other malicious, unsolicited e-mails sent to a recipient – such as urban legends, and the like – would not qualify as spam in Africa.

[205] Ibid.

While the SADC Model Law and the AU Convention appear to have provided an exhaustive list of definitions, the COMESA Model Law falls short in this regard. It is further worth noting that some of the terms that are important in clarifying the spam problem such as “marketing” or “online marketing” (used in the SADC Model Law and the AU Convention) are not defined.

5.4.2 Contrasting the instruments: mechanisms

As with any other spam legislation, the mechanism is always the most important element when it comes to regulating spam, and this is where the documents differ. Both the AU Convention and the SADC Model Law advocate a restrictive approach to spam in the form of the opt-in mechanism. These two instruments make the sending of spam illegal in their jurisdictions by providing that direct marketing is only permitted where the particulars of the addresses have been obtained directly from the consumers; and the recipients must have consented to be contacted through marketing instruments.[206] The SADC Model Law on Computer Crimes and Cybercrime also criminalises the transmission of multiple electronic messages within customer and business relationships.[207]

The COMESA Model Law advocates an opt-out mechanism which does not prohibit spam but merely regulates it as shown above. In addition, it makes no provision for the requirements regarding the functionality of the opt-out facility. The SADC Model Law requires a valid opt-out facility to be included where the recipient elects not to receive similar communications in the future.[208] The originator who fails to provide the recipient with an operational opt-out facility is guilty of an offence.[209]

5.4.3 Requirements for sending electronic communications

The SADC Model Law is the most comprehensive of the three instruments considered. Both the AU Convention and the SADC Model Law addresses the

[206] See art 4(4)(a) and (b) of the AU Convention contrasted with s 30(3) of the SADC Model Law.

[207] See s 19(2) of the SADC Model Law on Computer Crimes and Cybercrime.

[208] See s 30(1)(b) of the SADC Model Law.

[209] Id ss 30(3)(c) and (d) and 30(5).

requirement that spammers should not disguise (spoof) their headers.[210] This is in line with the ITU's recommendation as noted in Chapter 4 above. This will also minimise the aggravation experienced by receivers who are not able to locate the sender of spam e-mails. Clear penalties for contravention of these provisions are also provided.[211]

As noted above, participation by different stakeholders in combating spam is vital as spam is not only a national issue but a global one which demands a multi-pronged approach. The issue of involving consumers or those affected by this scourge should be a priority in these instruments. Education for all regarding the inner workings of the Internet could reduce the amount of spam sent to consumers. Only the AU Convention contains an article that deals with education in its provisions on cyber security.[212]

The ISPs also need to inform and educate their clients not only about their products, but also on the dangers which come with the use of these products. The AU Convention also addresses the issue of stakeholders partnering together to combat spam especially in relation to the prohibition on harvesting and the sale of lists. As has been noted, governments need to introduce the study of cybercrime or cyber security and or electronic communication skills at lower levels in grade school, so that by the time those learners are consumers they would have learned how to protect themselves and be savvy while surfing the net.[213] The need for cooperation must also be prioritised and the ITU, in partnership with ISOC and the ATU, needs to follow up on and implement the measures identified at their workshops.

5.5 Conclusion

Africa is indeed rising by aligning itself with the world on ICT laws. While there is still a long way to go, the first steps have been taken. Most countries in the African region have yet to implement laws regulating electronic commerce, personal data

[210] Id s 30(1)(a) and (b). Information such as: contact details; place of business; e-mail addresses; and telefax should be provided; art 4(1) of the AU Convention, and s 19(1)(c) of the SADC Model Law on Computer Crimes and Cybercrime.

[211] See s 30(8) of the SADC Model Law.

[212] See, in particular, art 26 of the AU Convention.

[213] See Chap 4 par 4.4.2.3 par (e) where the element of education is discussed.

protection, and cybersecurity. The instruments described above, with regards to the issue of spam, are of vital importance – more particularly in those jurisdictions which have yet to implement relevant legislation. For those that are in the process of doing so, the instruments will assist in the legislative drafting process. Those that already have laws in place can also benefit from these instruments by amending their legislation where necessary in order to tighten their control over spam. Where the national laws provide greater protection on the issue of spam, those nations should publicise their provisions so that the Convention or Model Laws can be amended accordingly.

In all three instruments member states or state parties are encouraged to ratify these instruments but only time will tell whether this will in fact happen. Be that as it may, these instruments are not binding on member states but are there as a guide for parties who embark upon the process of implementing ICT laws in their region, or to draw from the instruments those provisions that might enhance and strengthen their existing laws aimed at combating spam.

In the next three chapter’s focus will be on anti-spam laws in three jurisdictions to establish how those countries are dealing with the problem: Chapter 6 focuses on the USA; Chapter 7 on Australia; and Chapter 8 on the South African regulatory regime.

CHAPTER 6

A COMPARATIVE STUDY OF ANTI-SPAM LAWS: THE UNITED STATES OF AMERICA (USA)

6.1 Introduction

The preceding two chapters dealt with initiatives to combat spam at both the international and regional levels. In this and the following two chapters, focus will be on the national anti-spam laws in three countries: the USA, Australia, and South Africa. It should be noted that these countries' anti-spam legislation and provisions considered here were in place when the international initiatives were being conducted. At the time of writing it is estimated that, worldwide, there are over fifty countries with anti-spam laws or provisions.[1]

In this chapter focus will be on the anti-spam legislation in the USA. Before the USA passed its federal anti-spam law, most of the states had already implemented anti-spam legislation. It is consequently appropriate to consider anti-spam legislation from both the state and the federal perspectives. At state level an outline of anti-spam legislation focusing specifically on the requirements for the transmission of e-mail messages is provided. At federal level a commentary on the federal anti-spam law will be outlined with specific focus on: the benefits it offers; commentators' criticism levelled at certain of its provisions; and suggestions for improvement. This discussion includes an evaluation of relevant case law illustrating how the courts have interpreted specific provisions in both state and federal law.

6.2 Anti-spam laws at state level in the USA

6.2.1 Background

There are 52 states in the USA and all but twelve had anti-spam legislation in place before the federal law came into operation.[2] State laws were passed from 1997 until

[1] See Spamlaws 'Spam laws' http://www.spamlaws.com (date of use: 30 December 2015) for a list and brief summary of these anti-spam laws.

[2] States that had not enacted legislation relating to unsolicited bulk or commercial e-mail included: Alabama; Hawaii; Kentucky; Massachusetts; Mississippi; Montana; Nebraska; New

the enactment of the federal law in 2003.[3] These state laws differ as to what constitutes spam and how to regulate it.[4] Below is a discussion on anti-spam laws at state level.

6.2.2 Features of anti-spam laws at state level

6.2.2.1 Definition of spam in state laws

Anti-spam state laws use the following terms to describe spam: "unsolicited commercial electronic message or mail" (UCEM or UCE);[5] "unsolicited commercial mail advertisement" (UCEA);[6] "unsolicited bulk electronic e-mail" (UBEM or UBE);[7]

Hampshire; New Jersey; New York; South Carolina; and Vermont. See Kendrick (2003) 7/3 *Journal of Small and Emerging Business Law* 565.

[3] The first state to pass an anti-spam law was Nevada. See Nevada Revised Statutes (as amended in 2001 and 2003); also Prince & Shea (2003) 22 *John Marshall Journal of Computer & Information Law* 33-4 and 76.

[4] See, generally, Sorkin (2003) 22/1 *The John Marshall Journal of Computer and Information Law* 3 ff; also Nelson (2003) 58 *The Business Lawyer* 1209-10; and id Prince & Shea 33-40.

[5] "UCEM" means "a commercial e-mail message sent without the consent of the recipient, by a person with whom the recipient does not have an established business relationship". See s 44-1372 (6) of the Arizona Revised Statutes Title 44 Trade and Commerce Chapter 9 Trade Practices Generally art 16 Commercial e-mail (added by 2003 SB 1280 approved 16 May 2003 hereafter 'Arizona Revised Statutes'). UCEM also means "any commercial e-mail message that is not a transactional or relation message that is sent to a recipient without the recipient's affirmative or implied consent". See s 668.602(14) of the Florida Statutes Title 39 Commercial Relations Chapter 668 Electronic commerce Part III e-mail communications (added by 2004 Fla Laws ch 233 approved 25 May 2004 effective 1 July 2004), hereafter 'Florida Statutes'. In addition to these two states, other states also define spam as UCEM including: Louisiana; Missouri; Oregon; South Dakota; and Texas to mention but a few. UCE, on the other hand, means "an e-mail other than e-mail sent at the request of the recipient, via an e-mail service provider to two or more recipients in the state with whom the sender does not have an existing business relationship for the purpose of offering real property, goods or services". See s 45.50.479 (b)(3) of Alaska Statutes Title 45 Trade and Commerce Chap 50 Competitive Practices and Regulation of Competition s 479 Limitation of electronic mail (added by 2003 Alaska Laws ch 14 HB 82 2003 approved 5 May 2003 effective 30 July 2003), hereafter 'Alaska Statutes'; see too, s 1497(1)(C) of the Maine Revised Statutes: Title 10 Commerce and Trade Part 3 Regulation of Trade Chapter 224 Electronic Mail Solicitation (added by Public Laws ch 327 (2003) HB 210 approved May 2003), hereafter 'Maine Revised Statutes'. UCE is discussed below.

[6] "UCEA" means "a commercial e-mail advertisement sent to a recipient who meets the following criteria: the recipient has not provided direct consent to receive advertisements from the advertiser and the recipient does not have a pre-existing or current business relationship". See s 17529(o)(1-2) California Business and Professions Code Division 7 Part 3 Ch 1 art 1.8 Restrictions on Unsolicited Commercial E-Mail Advertisement (added by Stats 2003 ch 487 SB 186 approved 23 September 2003 as amended), hereafter 'California Business and Professions Code'; see too s 815 ILCS 511/5 Illinois Compiled Statutes ch 815 Business Transactions Deceptive Practices 815 ILCS 511/ Electronic Mail Act, hereafter 'Illinois Compiled Statutes'.

[7] "UBE/UBEM" means "any electronic message which is developed and distributed in an effort to sell or lease consumer goods and services and is sent in the same or substantially similar form to more than one thousand recipients". See ss 73.1 (13) and 73.6 of the Louisiana Revised

“unsolicited bulk commercial e-mail” (UBCE);[8] “unsolicited commercial or sexually explicit e-mail”;[9] or simply the “prohibition of e-mail with specific content”. The variations in state legislation above, define spam either as unsolicited commercial e-mail or communications (UCE), or unsolicited bulk e-mail (UBE).[10] These two variants are further discussed below.

(a) Unsolicited commercial e-mail (UCE)

An unsolicited commercial e-mail or message is classified as such “if it is sent to a person who does not have an existing personal or business relationship with the sender, and/or to a person who has not given permission for or requested the sending of the commercial e-mail”.[11] Sorkin raises a number of arguments in support of defining spam as UCE including:[12]

> the fact that spam shifts costs from the sender to the recipients; its use for commercial purposes is objectionable; that defining spam as UCE rather than UBE avoids the need to

Statutes Title 14 Criminal Law (as amended by 1999 La Acts 1180 approved 9 July 1999), hereafter ‘Louisiana Revised Statutes Title 14’; also s 39-14-603 (a) of the Tennessee Code Title 39 Criminal Offences Ch 14 Offenses against Property Part 6 Tennessee Personal and Commercial Computer Act of 2003 (added in 2003), hereafter ‘Tennessee Code’. UBE is discussed below.

[8] “UBCE” (or bulk e-mail advertisement) means “an electronic message, containing the same or similar advertisement, which is contemporaneously transmitted to two or more recipients, pursuant to an Internet or intranet computer network”. See s 48-603E (a) of the Idaho Code Title 48 Monopolies and Trade Practices Ch 6 Consumer Protection Act s 48-603E Unfair Bulk E-mail Advertisement Practices (added by House Bill 505 approved 17 April 2000 effective July 1 2000), hereafter ‘Idaho Code’; and s 1.75.4(4)(c) of the North Carolina General Statutes (as amended in 1999), hereafter ‘North Carolina General Statues’.

[9] “Sexually explicit e-mail” means “an e-mail that promotes or contains an electronic link to material that is harmful to minors”. See s 13-36-102(7)(a) of the Utah Code Title 13 Commerce and Trade Ch 36 Unsolicited Commercial and Sexually Explicit E-mail Act (added by Utah Laws 2002 Ch 125 and 229), hereafter ‘Utah Code’; also s 944.25(c) of Wisconsin Statutes Ch 944 Crimes against Sexual Morality (added by 2001 Act 16 approved 1 June 2001) hereafter ‘Wisconsin Statutes’; and s 4-88-602(11) of the Arkansas Code Title 4 Business and Commercial Law Subtitle 7 Consumer Protection Ch 88 Deceptive Trade Practices subchapter 6 Unsolicited Commercial and Sexually Explicit E-mail Prevention Act (added by Act 1019 of 2003 approved 2 April 2003), hereafter ‘Arkansas Code’.

[10] Sorkin (2001) 35/2 *University of San Francisco Law Review* 327-32; Kendrick (2003 Fall) 7/3 *Journal of Small and Emerging Business Law* 566-8 where the author discusses how states are split on the definition of spam.

[11] See s 45.50.479(b)(3)(A) and (B) Alaska Statutes; s 1497.1(c) Maine Revised Statutes; s 445.2502(h) of the Michigan Compiled Laws Ch 445 Trade and Commerce Unsolicited Commercial e-mail Protection Act (added by 2003 Mich Pub Act 42 HB 4519 effective 1 September 2003), hereafter ‘Michigan Compiled Laws’; and s 407.1120(2) of the Missouri Revised Statutes Title 26 Trade and Commerce Ch 407 Merchandising Practices E-mail Practices (enacted in 2000 amended by House Bill 228 (2003) approved 11 July 2003 effective 28 August 2003), hereafter ‘Missouri Revised Statutes’.

[12] See Sorkin (2001) supra n 10 334.

> establish a specific threshold for “bulk”; also that non-commercial messages (especially those of a political or religious nature) may constitute protected speech, while commercial messages can be regulated without falling foul of the First Amendment;[13] regulation limited to commercial messages stands a better chance of being adopted than regulation applicable to both commercial and non-commercial messages; and that existing legislation regulating commercial telephone and facsimile solicitation, could easily be extended to cover commercial solicitation transmitted by e-mail.

While the arguments for UCE are valid, certain commentators are of the view that there is a danger – apart from the risks of censorship and breach of confidentiality of communication – in defining spam by content.[14] The burden of spam should not be defined by its commercial nature *per se* in that non-commercial messages present as many problems as their commercial counterparts.[15]

(b) Unsolicited bulk e-mail (UBE)

The term UBE is defined as any electronic message which is “developed and distributed in an effort to sell or lease consumer goods or services, and is sent in the same or substantially similar form to more than 1 000 recipients”.[16] To qualify as “bulk” the required number of copies of messages sent must be within a certain time period.[17] Others define UBE as Internet mail sent to a group of recipients who have not requested it.[18] According to Spamhaus, spam is about “consent” not “content” (in

[13] The First Amendment is one of the ten Amendments that comprise the Bill of Rights in the USA. These Amendments were adopted on 15 December 1791. The First Amendment prohibits the making of any law respecting an establishment of religion, impeding the free exercise of religion, abridging the freedom of speech, infringing freedom of expression et cetera. See Dictionary.com ‘First Amendment’ http://www.dictionary.reference.com/browse/first-amendment (date of use: 30 December 2015).

[14] Asscher & Hoogcarspel *Regulating Spam* 11.

[15] Ibid.

[16] See ss 73.1(13) and 73.6 of the Louisiana Revised Statutes Title 14; s 48-603E(a) of the Idaho Code; s 18.2-152.3:1(B)(1-2) of the Virginia Code Title 18.2 Crimes and Offenses Generally Ch 5 Crimes against Property article 7.1 Computer Crimes (including amendments by Acts 2003, ch 987 & 1016, approved 3 April 2003), hereafter ‘Virginia Code’. Sorkin (2001) supra n 10 330-2 opines that “there is no generally agreed number of e-mails and that there is some resistance in the anti-spam community to establish or disclose a precise number”.

[17] Ibid. In terms of this section “the volume of UBE transmitted to recipients should exceed 10000 attempts in any 24 hour period; 100000 attempts in any 30 day time period; or one million in any year time period”. See too, s 48-603E (d) (4) of the Idaho Code.

[18] Hoffman P ‘Unsolicited bulk e-mail: definitions and problems’ http://www.imc.org/ube-def.html (date of use: 30 December 2015); TechTarget ‘UBE (unsolicited bulk email) definition’ http://searchcio.techtarget.com/definition/UBE where the defining characteristics of UBE are listed as being sent as a mass mailing to a huge number of recipients at a time; and at least some of the intended recipients have not agreed to receive messages from the sender (date of use: 30 December 2015); Daniels J ‘Bulk e-mail or opt-in’ http://www.icontact.com/static/pdf/Bulk-E-mail.pdf (date of use: 30 December 2015); and Clayton R ‘Good practice for combating unsolicited bulk e-mail’ http://www.ripe.net/ripe/docs/ripe-206 (date of use: 30 December 2015).

other words, recipients must have consented to receive the mail regardless of the content of the message).[19] Whether the unsolicited bulk e-mail message is an advert, a scam, or whatever, is irrelevant if the message was unsolicited and sent in bulk.[20]

Arguments raised for defining spam as UBE include:[21]

(a) The primary argument for defining spam as UBE is simply that the commercial or non-commercial nature of an unsolicited message has little or nothing to do with the damage that is inflicted. The problem is not that the costs are shifted from the sender to recipients, but merely that recipients, and intermediate networks, sustain costs involuntarily, making the sender's motivation largely irrelevant;

(b) A legal rule against all unsolicited bulk e-mail is arguably more content-neutral than a rule that focuses on commercial messages. A rule focusing only on commercial messages might well open the floodgates to a massive increase in non-commercial spam. Since the problem with spam is volume and not content, the UBE approach seems to make more sense;

(c) Restricting all unsolicited e-mail, rather than merely UCE or UBE, is probably not a realistic option. Single or non-commercial, unsolicited messages are far less objectionable than UCE or UBE and a much stronger case can be made for constitutional protection of such messages than for either UCE or UBE; and

(d) A fourth alternative would be to limit the definition to messages that are both commercial and sent in bulk, "UBCE"[22] for short. Since nearly all UCE is sent in bulk, this approach is roughly equivalent to defining spam as UCE, though it would be accompanied by the same evidentiary difficulties as the UBE definition.

What emerges from the discussion above is that there are two clear camps on how spam should be defined. Below is an outline of the nature of spam flowing from the definitions above.

(c) The nature of spam

The following elements of spam can be isolated: unsolicited; commercial; and bulk.[23] While commentators agree on the "unsolicited" element, they differ when it comes to the type of mail involved – for example, whether the focus should be on "content" or on the "volume" of the e-mail message sent. The following is a brief description of these elements.

[19] Spamhaus 'The definition of spam' http://www.spamhaus.org/consumer/definition (date of use: 30 December 2015).

[20] Ibid.

[21] See Sorkin (2001) supra n 10 335.

[22] See supra n 8 for the definition of UBCE.

[23] These elements are sometimes referred to as: "key aspects" (see, in particular, Sorkin (2001) supra n 10 328); "keyword" see Asscher & Hoogcarspel supra n 14 10.

Unsolicited

In order to qualify as spam the communication or e-mail must be unsolicited. Some states have defined unsolicited to mean without the recipients' express permission – save that commercial e-mail is not unsolicited if the sender has a pre-existing business[24] or personal relationship with the recipient(s).[25] An e-mail is also not unsolicited if it was received as a result of the recipient opting into a system in order to receive promotional material.[26] Therefore, unsolicited means "not addressed to a recipient with whom the initiator has an existing business or personal relationship, and not sent at the request of, or with the express consent of the recipient".[27] In addition to the unsolicited element, other elements depend on either the content or volume of the communication. [28]

Commercial

Commercial is generally classified in terms of the message content rather than "the sender's actual or presumed reason for sending the message".[29] This term therefore includes messages that promote the sale of goods or services, and/or the exchange of goods, services or real property.[30] It also means any e-mail message sent to a

[24] "Pre-existing" or "current business relationship" as used in connection with the sending of commercial e-mail provides that "the recipient has made an inquiry and has provided his or her e-mail address, or has made an application, purchase, or transaction, with or without consideration regarding products or services offered by the advertiser". See s 16-9-100(17) of the Official Code of Georgia Title 16 Crimes and Offences Ch 9 Forgery and Fraudulent Practices art 6 Computer Systems Protection (as amended by Senate Bill 62 2005, approved and effective 19 April 2005), hereafter 'Official Code of Georgia'; and s 17529(l) of the California Business and Professions Code. A "pre-existing business relationship" also means that "there was a business transaction between the initiator and the recipient of a commercial electronic mail message during the five year period preceding the receipt of that message. This includes transactions involving the free provision of information, goods, or services requested by the recipient, and it does not exist after a recipient requests to be removed from the distribution lists of the initiator". See s 2307.64(8) Ohio Revised Code Title 23 Courts Common Pleas Ch 2307 Civil Actions Damage and Theft (as amended by HB 361 2005 effective 6 May 2005), hereafter 'Ohio Revised Code'.

[25] See s 4-88-602(12) of the Arkansas Code; also s 445.2502.2(h) of the Michigan Compiled Laws; and s 13-36-102(8)(a) of the Utah Code.

[26] See s 445.2502.2(h) of the Michigan Compiled Laws.

[27] See s 14-453(10) of the North Carolina General Statues.

[28] See Warner (2003) 22/1 *John Marshall Journal of Computer & Information Law* 156 where the author differentiates between the two types of approach, namely excess (volume) and the content-based approach.

[29] Sorkin (2001) supra n 10 329-30.

[30] See s 4-88-601(1) of the Arkansas Code; and s 776.4(5) of the Oklahoma Statutes Title 15 Contracts (added by Okla. Laws 1999 ch 337 House Bill 1410 1999 approved 8 June 1999

receiving address or account and aimed at advertising,[31] promoting, marketing, or otherwise attempting to solicit interest in any goods, services, or enterprise.[32] The term commercial does not mean an e-mail message to which an interactive computer service provider has attached an advertisement in exchange of free use of an e-mail account where the sender has agreed to such an arrangement.[33]

Sorkin notes that communications such as newsletters, chain letters, opinion surveys, and urban legends will not be regarded as spam as they lack "commercial content", although they may satisfy the "bulk" element if they are sent to a sufficient number of recipients. [34]

Bulk

A bulk e-mail refers to an e-mail containing the same advertisement or message being transmitted to two or more recipients using an Internet or intranet computer network.[35] The bulk element is referred to by some as "the excessive volume approach which avoids content by insisting that content is irrelevant in deciding whether an e-mail qualifies as spam".[36] Haase[37] et al are of the opinion that the bulk of spam messages share one or more of the following characteristics:

effective 1 July 1999 amended by Senate Bill 660 2003 effective 1 November 2003), hereafter 'Oklahoma Statutes'.

[31] "Advertising" means an "electronic mail message sent to a computer for the purpose of promoting real property, goods, or services for sale, lease, barter, or auction". See s 714E.1 (a) of the Iowa Code Ch 714E (added by House File 448 (1999) approved 26 May 1999 effective 1 July 1999), 'hereafter 'Iowa Code'; s 41.710 of the Nevada Revised Statues; also see the following states: Georgia; Kansas; Maryland; North Dakota; Oklahoma; Oregon; Pennsylvania. Also see Warner (2003) supra n 28 156.

[32] See s 931(17) of the Delaware Code Title 11 Crimes and Criminal Procedure (as amended by 72 Del Laws ch 135 approved 23 June 1999 effective 2 July 1999), hereafter 'Delaware Code'; s 51.1741(1); Louisiana Revised Statutes Title 51 Trade and Commerce Ch 19-C Unsolicited Commercial E-mail Restrictions (added by 2003 La Acts 1275 approved 2 July 2), hereafter 'Louisiana Revised Statutes Title 51'.

[33] See s 40-12-401(a)(ii) of the Wyoming Statutes Title 40 Trade and Commerce Ch 12 Consumer Protection art 4 Commercial Electronic Mail (added by 2003 Wyo Laws ch 86 approved 3 March 2003 effective 1 July 2003), hereafter 'Wyoming Statutes'; and s 932(17) of the Delaware Code.

[34] Sorkin (2001) supra n 10 333-6.

[35] See s 48-603E (a) of the Idaho Code.

[36] See Warner (2003) supra n 28 156; Dickinson (2004) 57/1 *Federal Communications Law Journal* 151; Asscher & Hoogcarspel supra n 14 10.

[37] Haase, Grimm & Versfeld *International Commercial Law* 131-5; also s 73.6 Louisiana Revised Statutes Title 14; s 39-14-603(a) of the Tennessee Code; and s 18.2-152.3:1(B) of the Virginia Code.

> (a) They include or promote illegal or offensive content;
> (b) Their purpose is fraudulent or otherwise deceptive;
> (c) They are sent in a large untargeted and indiscriminate manner, often by automated means;
> (d) They are sent in a manner disguising the originator;
> (e) They do not offer a working address to which the recipient may send messages opting-out of receiving further unsolicited messages; and
> (f) They could collect personal information in breach of recipients' privacy. These characteristics are not essential to whether an electronic message should be regarded as unsolicited or sent in bulk.

From the above, it is clear that the definition of spam has three different elements, and depending on which state law one consults, those elements will apply in defining spam. It is also clear that one commercial e-mail sent to a number of recipients can be regarded as spam e-mail and can also satisfy the bulk requirement. In addition to the definitions above, state laws have mechanisms in place to regulate spam.

6.2.2.2 Mechanisms to regulate spam

As noted in Chapter 4, there are two mechanisms used to regulate spam in anti-spam legislation: the opt-in and opt-out mechanisms. The following is a brief description of these mechanisms as provided in state laws.

(a) Opt-in mechanism

Only a handful of state laws use opt-in as a mechanism to regulate spam.[38] Opt-in requires prior consent from the recipient before any marketing correspondence can be sent to him or her.[39] Grossman notes that "the opt-in mechanism generally manifests in two ways: a mechanism that rigorously requires that a potential recipient give specific assent to receiving a specific communication; and a less stringent form which infers permission from established relationships".[40] Concepts such as: pre-existing relationship;[41] direct consent;[42] established business;[43] or affirmative

[38] Only two states have adopted an opt-in approach namely: California and Delaware.

[39] This prohibits unsolicited communications to be sent without prior relationship. See Grossman (2004) 19/4 *Berkeley Technology Law Journal* 1547-8.

[40] Ibid. The "less stringent forms" means "a previous established relationship between the individual and the retailer, whereby that individual had bought or contacted that retailer before communications were sent".

[41] See supra n 24 for a definition of pre-existing relationship.

[42] "Direct consent" provides that "the recipient has expressly consented to receive e-mail advertisements from the advertiser, either in response to a clear and conspicuous request from

consent[44] describes this mechanism. The state of California prohibits a person or an entity from initiating or advertising in an unsolicited commercial e-mail advertisement from and to a state.[45] California's state law also provides that: [46]

> commercial e-mail advertisements sent pursuant to the exemption allowed for a pre-existing or current business relationship, shall provide the recipient of that commercial e-mail advertisement with the ability to opt-out from receiving further commercial e-mail advertisements by either calling a toll free number or by sending an unsubscribe e-mail to the advertiser offering the products or services in that advertisement. The opt-out provision does not apply to recipients who are receiving free e-mail service with regard to commercial e-mail advertisements sent by the provider of the e-mail service.

Delaware on the other hand, makes it unlawful for any person to send "un-requested" or "unauthorised" e-mail to another person, and also discourages the distribution (intentionally or recklessly) of any unsolicited bulk commercial e-mail to a receiving address or account under the control of an authorised user of a computer system.[47]

Ledbetter[48] notes that while this mechanism greatly reduces the amount of spam by criminalising even a single attempt by a marketer to solicit consent, it is not without its problems.[49] It has been argued that the California statute shuts down "permission-

the consent or at the recipients own initiative". See s 17529.1(d) of the California Business and Professional Code; and s 16-9-100(4) of the Official Code of Georgia.

[43] The term "established business relationship" means "a prior existing relationship formed by a voluntary communication between a person or entity and the recipient with or without an exchange of consideration, on the basis of an inquiry, application, purchase or use by the recipient regarding products or services offered by the person or entity". See s 44-1372(4) of the Arizona Revised Statutes; also s 776.5(3) of the Oklahoma Statutes; and s 2250.2(2) of the Pennsylvania Statutes Title 73 Trade and Commerce Ch 40A Unsolicited Telecommunication Advertisement Act (added by 2002 Pa Laws 222 approved 16 December 2002), hereafter 'Pennsylvania Statutes'.

[44] "Affirmative consent" means that "the recipient of e-mail expressly consented to receive the message either in response to a clear and conspicuous request for the recipients' consent or the recipients own initiative. A recipient is deemed to have given affirmative consent if the e-mail message is from a person other than the person to whom the recipient directly communicated consent if clear and conspicuous notice was given to the recipient that the recipients e-mail address could be transferred to another person for the purpose of that person initiating the transmission of commercial e-mail message to the recipient". See s 668.602(1) of the Florida Statutes.

[45] See s 17529.2(a) and (b) of the California Business and Professions Code; and s 668.603(1) of the Florida Statutes.

[46] Id s 17529.1(l) of the California Business and Professions Code.

[47] See s 937(a) of the Delaware Code. This section does not apply to e-mail that is sent between human beings, or when the individual has requested the information.

[48] See Ledbetter (2004) 34 *Southwestern University Law Review* 122.

[49] Ibid.

based" e-mail lists between marketers, regardless of a consumer's willingness to give permission.[50]

(b) Opt-out mechanism

The bulk of anti-spam laws at state level in the USA have implemented the opt-out mechanism as part of their regulation of spam. The opt-out mechanism advocates that the sender[51] may send spam messages to consumers even if there is no existing relationship between the two. The sender must provide the recipient[52] with a convenient opt-out facility and a cost-free mechanism by which to notify the sender not to send any future e-mail(s) to the recipient.[53] However, this mechanism must include[54] a valid functional return e-mail address.[55] In addition to this, sexually explicit e-mail(s) should also include a toll-free telephone number, if the sender has one.[56] The sender must also maintain a functioning web site at which a recipient may request his or her removal from the sender's mailing list.[57]

Once the sender has been notified of the opt-out request, that sender must do the following: stop sending unsolicited e-mails to all of the e-mail addresses registered to the person who sent the request or entity opting out directly or indirectly through third

[50] Ibid.

[51] The term "sender" means "a person who initiates a commercial e-mail advertisement". See s 51:1741(13) of the Louisiana Revised Statutes Title 51; and s 46.001(7) of the Texas Statutes Title 4 Business & Commerce Code Ch 46 e-mail Solicitation (added by Act 2003 ch 1053 House Bill 1282 approved 20 June 2003 effective 1 September 2003), hereafter 'Texas Statutes'.

[52] The term "recipient" means "the addressee of an unsolicited commercial e-mail advertisement. If an addressee of a commercial e-mail advertisement has one or more e-mail addresses to which a commercial e-mail advertisement is sent, the addressee shall be deemed to be a separate recipient for each address to which the advertisement is sent". See s 17529.1(m) of the California Business and Professional Code; also s 16-9-100(19) of the Official Code of Georgia; and s 51.1741(12) of the Louisiana Revised Statutes Title 51.

[53] See s 4-88-603 of the Arkansas Code; s 445.2502(h) of the Michigan Compiled Laws; s 776.6 (E) of the Oklahoma Statutes; and s 46.003(2) of the Texas Statutes.

[54] See s 51:1741.1 of the Louisiana Revised Statutes Title 51; and s 1497(2) of the Maine Revised Statutes.

[55] The phrase "functioning return e-mail address" means "an e-mail address displayed in a commercial e-mail advertisement that has the capacity to receive the number of reply messages that the sender of the commercial e-mail advertisement should reasonably expect to be transmitted by the recipients for no less than thirty days after the sending of such advertisements". See s 51:1741(6) of the Louisiana Revised Statutes Title 51.

[56] See s 4-88-603 (3) (a), (b); and (4) of the Arkansas Code; also s 13-36-103 (1) (c) (ii) of the Utah Statutes; and s 445.2503 93 of the Michigan Compiled Statutes.

[57] See s 51.174.1(2) of the Louisiana Revised Statutes Title 51.

parties;[58] and remove the recipient's e-mail address from its e-mail list not later than the third day after the date on which the sender receives a request for removal of that address.[59] The sender must also establish and maintain the necessary policies and records to ensure that a recipient who has notified the sender of such request that he or she no longer wishes to receive further mail, in fact does not receive any e-mail from the date of the notice.[60] In addition to the above, the sender should update its records not less than fourteen business days after such request.[61]

6.2.2.3 Labelling of e-mail messages

Most state laws require that an unsolicited e-mail containing advertisements should include the following in its subject line: "ADV" as the first four characters;[62] and "ADV: ADLT" as the first eight or nine characters (or in the first word) if the message contains information consisting of explicit sexual material that may only be viewed or purchased by an individual of eighteen years of age or older.[63] In addition to the above, certain states require attorneys who advertise via unsolicited e-mail to include "legal advertisement" in the subject line[64] together with "THIS IS AN

[58] See s 1497(2) of the Maine Revised Statutes and s 445.2504 (2) of the Michigan Compiled Laws.

[59] See s 46.003(b) of the Texas Statutes.

[60] See s 445.2504(3) of the Michigan Compiled Laws.

[61] Ibid.

[62] "ADV" stands for advertising or advertisements. Most of these advertisements usually include unsolicited advertising material for the lease, sale, rental, gift, offer et cetera. See s 52-570c.(b) of the General Statutes of Connecticut Title 52. Civil Actions chapter 925. Statutory Rights of Actions and Defences (as amended in 2003); s 668.603.(1)(c) and (d) of the Florida Statutes; s 50-6-107(c)(1)(C) of the Kansas Statutes Ch 50 Unfair Trade and Consumer Protection art 6 Consumer Protection (added by Laws 2002 ch 140 (SB 467 approved 17 May 2002); s 51.1741.1(4) Louisiana Revised Statutes Title 51; s 1497(3)(1) of Maine Statutes; s 57-12-23(3) of the New Mexico Statutes Title 57 Trade and Commerce art 12 Unfair Practices Act (added by 2003 SB 699 2003 NM Acts ch 168 approved 5 April 2003); s 41.725 (2) of the Nevada Statutes; s 776.5(6)(C) of the Oklahoma Statutes; s 37-24-6(13) of the South Dakota Codified Laws Ch 37-24 Deceptive Trade Practices and Consumer Protection provisions added or amended in 2002), hereafter 'South Dakota Codified Law'; s 47-18-2501(e) of the Tennessee Code; and s 13-36-103(1)(b) of the Utah Statutes.

[63] States that have these provisions include among others: s 50-6-107(c)(1)(E) of the Kansas Statutes; s 51.1741.1(5) Louisiana Revised Statutes Title 51; s 1497(3)(2) of Maine Statutes; s 4-88-603(a)(2); s 57-12-23(4) of the New Mexico Statutes; s 51-27-04(1) of North Dakota Statutes; s 776.5(6)(D) of the Oklahoma Statutes; s 37-24-6.(13) of the South Dakota Codified Laws; s 47-18-2501(e) of the Tennessee Statutes; s 13-36-103(1)(b) Utah Code; and s 944.25(1) and (2) Wisconsin Statutes; and s 46.003 (a) of the Texas Statutes.

[64] See Florida Rules of Professional Conduct (Fla RPC) rule 4-7.6(c)(3) http://www.law.cornell.edu/ethics/fl/code/FL_CODE.HTM (date of use: 30 December 2015) dealing with computer accessed communications; also Spamlaws 'SpamLaws' http://www.spamlaws.com/state/summary.shtml (date of use: 5 January 2016).

ADVERTISEMENT" prominently in each communication.[65] These e-mail messages must also clearly and conspicuously disclose the following sender information: its legal name; correct street address; valid Internet domain name; and a valid return e-mail address.[66] Kendrick[67] notes the following regarding the requirement of placing "ADV" on the header of an e-mail:

> that this will afford consumers an opportunity to decide whether to read or discard the message; furthermore, that the Internet marketplace will move away from support for many small businesses towards a market that supports only a few established businesses; that the standardised ADV label will be used as a flag for ISPs and users to establish e-mail filters to either block or immediately delete the messages, which will, in turn, block new products or new providers, and so benefit established marketers or online providers who have already captured the attention of consumers; and that labelled messages are also said to stigmatise the message to a degree difficult for an emerging business to overcome in that the label will in time become synonymous with, for example, pornography, shady businesses, financing deals, and the like.[68]

6.2.2.4 Falsified or misleading headers and information

(a) Background

Most states prohibit individuals from transmitting commercial e-mail messages which intentionally falsify[69] headers or other routing information of unsolicited commercial e-mail messages. This provision also prohibits e-mail messages[70] that: contain false,

[65] In the state of Kentucky, attorneys who advertise via written, recorder, or electronic communication targeted at potential clients, are required to display those words in capital letters. See SCR 3.130(7.09) of the Kentucky Bar Association Rules of the Supreme Court of Kentucky (Ky Sup Ct) http://www.cle.kybar.org/documents/scr/scr3/scr_3.130_(7.09).pdf (date of use: 5 January 2016).

[66] See s 51:1741.1 (3)(a)-(c) of Louisiana Revised Statutes Title 51; and s 13-36-103.(1)(d) of the Utah Statutes.

[67] Kendrick (2003 Fall) supra n 10 574; also Bolin (2006) 24/2 *Yale Law and Policy Review* 415-17.

[68] Ibid Kendrick.

[69] The term "materially falsified" means "altered or concealed in a manner that would impair the ability of one of the following to identity, locate or respond to a person who initiated an e-mail message to investigate an alleged violation of the section; a recipient of the message; an Internet access service processing the message on behalf of the recipient; a person alleging a violation of the section; or a law enforcement agency" (see s 3-805.1(10) of the Maryland Criminal Law Code Title 3 Other Crimes Against the Person Subtitle 8 Stalking and Harassment (as amended in 2004), hereafter 'Maryland Criminal Law Code').

[70] 'Electronic mail message' means "an electronic message or computer file that is transmitted between two or more telecommunications devices; computers; computer networks, regardless of whether the network is a local, regional, or global network; or electronic devices capable of receiving electronic addresses, regardless of whether the message is converted to hard copy format after receipt, viewed upon transmission or stored for later retrieval". The term "e-mail address", on the other hand, means "a destination commonly expressed as a string of

deceptive, or misleading information in their subject line;[71] use a third party's Internet domain name[72] without the permission of that third party; and fraudulently misrepresent or obscure any information identifying the point of origin or the transmission path of that commercial e-mail message.[73] The header information[74] or content of the commercial e-mail sent without authorisation and with intent to mislead must contain a personal name, entity name, trade name, mark, domain, address, and phone number of the sender.[75] A person shall "not knowingly sell, give, or otherwise distribute or possess with the intent to sell, give, or distribute, software for the purpose of facilitating or enabling the falsification of commercial e-mail transmission information or other routing information".[76] There have been a number of cases dealing with the falsification of headers and a selection is considered below.

(b) Selected case law

Parker v CN Enterprises

characters to which e-mail may be sent or delivered" (see s 668.601(6) and (7) of the Florida Statutes; s 16-9-100(7) Official Code of Georgia; and s 741E.1 (d) of the Iowa Statutes).

[71] "False and misleading" when used in relation to a commercial e-mail means that "the header information includes an originating or intermediate e-mail address, domain name, protocol address which was obtained by means of false or fraudulent pretences or representation; the header information fails to accurately identify the computer used to initiate the e-mail; the subject line of the e-mail is intended to mislead a recipient about a material fact regarding the content or subject matter of the mail; the header information is altered or modified in a manner that impedes or precludes the recipient of the e-mail or e-mail service provider from identifying, locating or contacting the person who initiated the e-mail". See s 16-9-100(10) (A)-(G) of the Official Code of Georgia; and s 1497(5) Maine Statutes.

[72] "Internet domain name" is defined as "a globally unique, hierarchical reference to an Internet host or service, assigned through centralized Internet naming authorities, comprising a series of character strings separated by periods with the right-most string specifying the top of the hierarchy". See s 407.1120(6) of the Missouri Revised Statutes; and s 37-24-36(6) of the South Dakota Codified Laws; and s 46.001(9) of the Texas Statutes.

[73] See s 6-47-2(d) of the Rhode Island General Laws Title 6 Commercial Law General Regulatory Provisions Chapter 47 Internet Access and Advertising by Facsimile (added in 1999), hereafter 'Rhode Island General Laws'; s 46.002 of the Texas Statutes; and s 19.190.020 of the Revised Code of Washington Title 19 Business Regulations-Miscellaneous Ch 19.190 Commercial Electronic Mail (as amended by 2003 Acts ch 137 HB 2007), hereafter 'Revised Code of Washington'.

[74] The term "header information" means "the source, destination, and routing information attached to an e-mail message, including the originating domain name and originating e-mail address, and any other information that appears in the line identifying or purporting to identify a person initiating the message, and technical information that authenticates the sender of an e-mail message for network management purposes". See s 3-805.1(6) of the Maryland Criminal Code and s 2913.421(A)(7) of the Ohio Revised Code.

[75] See s 16-9-100(10)(e) of the Official Code of Georgia.

[76] See s 445.2505(5) of the Michigan Compiled Laws. Other include the fact that it has only limited commercially significant purpose or use other than to facilitate or enable the falsification of commercial e-mail transmission information or other routing information.

The facts in *Parker v CN Enterprises*[77] were briefly that Nowak used a domain name (flowers.com) owned by Parker to send unsolicited mass mailings (spam) consisting of free cash grants of $19.95.[78] The court ordered that Nowak (his company and those acting in concert with him) refrain from using Parker's domain name in any e-mail, or from using any Internet domain name as a return address without the owner's permission.[79]

Kleffman v Vonage Holdings Corp

The facts in *Kleffman v Vonage Holdings Corp*[80] were briefly that Kleffman received unsolicited e-mail advertisements from eleven different domain names all advertising Vonage and its broadband telephone service.[81] Vonage was not specified in the domain name as the sender instead, the sender used other 'nonsensical' domain names.[82] The court held that "commercial e-mail advertisements sent from multiple domain names with the intent to bypass spam filters were not rendered unlawful by the California Business and Professionals Code".[83] The legal significance of this decision has been noted as "able to prevent the flood of potential litigation from other members of the public who are simply annoyed, unhappy, or bothered by the amount of commercial e-mail advertisements received on a daily basis, in that the legislation only governs and punishes those who send falsified or fraudulent e-mails".[84]

Commonwealth of Virginia v Jeremy Jaynes

[77] *Parker v CN Enterprises* (case no. 97-06273 Texas Travis County District Court (November 1997)) http://www.loudy.com/CASES/Parker_v_CN_Entterprises.html (date of use: 30 December 2015). Hereafter '*Parker's case*'.

[78] Nowak's spam used Parker's domain name in the electronic return address, which allowed Nowak to avoid receiving thousands of return-to-sender messages and the inevitable hate mail from recipients. As a result, Parker received thousands of such messages which prevented her from accessing her Internet account for hours and temporarily shutting down her ISPs mail servers. Ibid.

[79] Ibid.

[80] See *Kleffman v Vonage Holdings Corp* 232 P3d 625, 627 (Cal 2010) http://www.caselaw.findlaw.com/ca-supreme-court/1527999.html (date of use: 5 January 2016). Hereafter '*Kleffman's case*'.

[81] Ibid.

[82] Ibid.

[83] Section 17529.5(a) (2) of the California Business and Professional Code makes it unlawful to advertise in a commercial e-mail advertisement that contains or is accompanied by falsified, misrepresented, or forged headers.

[84] See *Kleffman's case* supra n 80; and for a discussion of this case see Machacek (2011) 14 *Chapman Law Review* 587.

The facts in *Commonwealth of Virginia v Jeremy Jaynes*[85] are briefly that in 2003 Jaynes used computers in his North Carolina home to send more than 10 000, (and in one instance over 20 000), unsolicited bulk e-mail messages with falsified routing and transmission information to America Online (AOL) proprietary network on three different occasions.[86] These messages were sent in bulk so contravening the Virginia Code.[87]

The respondent argued that the Virginia Code violated the First Amendment because it was overboard and the language prohibited anonymous speech of a non-commercial nature which is protected by the First Amendment.[88] Jaynes appealed his conviction on the basis of a "facial challenge"[89] to the statute. The court found that the statute used to charge Jaynes did not violate the First Amendment as it did not regulate free speech, and was not unconstitutionally vague in that it was not so vague that a person of ordinary intelligence could fail to understand its meaning.[90] The court also noted that the statute ciminalised the sending of bulk e-mail anonymously, and acknowledged that commercial bulk e-mail might constitutionally be regulated in that manner.[91] It also found that the statute extended beyond this to encompass non-commercial bulk e-mails.[92] Jaynes was convicted on three counts

[85] *Commonwealth of Virginia v Jeremy Jaynes* (case no 08-765) 1-31 http://www.scotusblog.com/wp-content/uploads/2009/03/08-765_bio.pdf (date of use: 30 December 2015). Hereafter '*Jaynes case*'.

[86] Id at 1-2. AOL is an ISP that provides e-mail accounts as part of its services located in Virginia. Each message was targeted at AOL subscribers as all e-mail addresses ended with "@aol.com". Jaynes also registered numerous different domain names using false contact information through Network Solutions, whose offices are located in Virginia.

[87] Section 18.2-152.3.1 of the Virginia Code provides for transmission of unsolicited bulk electronic mail.

[88] See *Jaynes case* supra n 85 2-3.

[89] "Facial challenge" is defined as "a challenge which claims that the law is unconstitutional on its face" (in this case the Virginia Code). See Kreit (2010) 18/3 *William & Mary Bill of Rights Journal* 657 http://scholarship.law.wm.edu/cgi/viewcontent.cgi?article=1168&context=wmborj (date of use: 30 December 2015).

[90] See *Jaynes case* supra n 85 15-30.

[91] Ibid.

[92] Id 3. Also see Meyerowitz (2008) *Privacy & Data Security Law Journal* 1024-42 http://www.meyerowitzcommunications.com/pdf/Meyerowitz%20Spam%20Ruling.pdf (date of use: 30 December 2015) especially 1035-9 where the author discusses the constitutionality of s 18.2-152.3:1 of the Virginia Code and other matters; Canfield (2010) 20 *Civil Rights Law Journal* 449 ff; and *Balsam v Trancos Inc* 2012 WL 593703 1-5 (Ca Ct App 24 2012) http://blog.ericgoldman.org/archives/2012/02/california_appe_2.htm (date of use: 30 December 2015).

and sentenced to three years' imprisonment on each count to run consecutively for a period of nine years.[93]

6.2.2.5 Harvesting and sale of lists and the use of dictionary attacks

(a) Harvesting of lists

Some states make it unlawful for any person or entity to collect e-mail addresses posted on the Internet if the purpose of the collection is to use those e-mail addresses either to initiate or to advertise in an unsolicited manner to a particular state.[94] It has been indicated elsewhere that because e-mail harvesting is generally automated, spam can hit the addresses soon after they are used publicly for the first time.[95]

(b) Selling or transferring lists

In certain states anti-spam legislation makes it unlawful for any person to knowingly sell or otherwise provide lists of e-mail addresses used to initiate the transmission of unsolicited commercial e-mail advertisements in violation of a particular state's law.[96] Only a few states provide for a procedure which allows recipients to restrict the future sale or transfer of their e-mail address information to another person or organisation for the purpose of sending commercial e-mail.[97]

[93] Ibid Meyerowitz; and *Jaynes case* supra n 85 15-30.

[94] See s 17529.4(a) (1) and (2) of the California Business and Professions Code and s 51.1741.2 (B)(1) and (2) of the Louisiana Revised Statutes Title 51.

[95] See FTC Consumer Alert 'E-mail address harvesting: how spammers reap what you sow' (November 2002) http://www.webmaestro.biz/pdf/addressharvesting.pdf (date of use: 30 December 2015). The Federal Trade Commission conducted an investigation into how spammers harvest e-mail addresses. "They "seeded" 175 different locations on the Internet with 250 new, undercover e-mail addresses. The locations included web pages, news groups, chat rooms, message boards, and online directories for web pages, instant message users, domain names, resumes and dating services. During the six weeks after those postings, the accounts received 349 spam e-mails; 86% of the addresses posted to web pages and newsgroups received spam. It did not matter where the addresses were posted on the page. If the address had the "@" sign in it, it drew spam; chat rooms were found to be virtual magnets for harvesting software. One address posted in a chat room received spam e-mails nine minutes after it was first used".

[96] See s 44-1372.01(B)(2)(b) of the Arizona Revised Statutes; s 51.1741.2(B)(1) and (2) of the Louisiana Revised Statutes Title 51; and s 445-2505(5) of the Michigan Compiled Laws.

[97] Ibid Arizona Revised Statutes; s 3.805.1 of the Maryland Criminal Law Code; and s 2250.4 (5) of the Pennsylvania Statutes.

(c) Dictionary attacks

State laws also prohibit the use of e-mail addresses obtained by automated means based on a combination of names, letters, or numbers to initiate or advertise in an unsolicited commercial e-mail from a particular state or advertisement sent from that state.[98] In addition to this, it is also unlawful for any person to use scripts or other automated means to register for multiple e-mail accounts from which to initiate or advertise, or to enable another person to initiate or advertise unsolicited commercial e-mail sent to and/or from a particular state.[99]

6.2.2.6 Enforcement and penalties

State laws advocate for both civil and criminal charges against those who violate certain of the provisions above.

(a) Criminal action

According to state laws, any transmission of unsolicited commercial or sexually explicit e-mail in violation of the provisions above constitutes an unfair and deceptive act or practice.[100] The prosecuting attorneys of various districts and counties in some states also have full authority to enforce the provisions of the sub-chapters in the laws.[101]

It is also an offence for a person intentionally to send a message(s) containing obscene material or material depicting sexual conduct in violation of the requirement that the “ADV” label appear on those particular e-mails.[102] Any person violating this provision regarding the sending of unsolicited commercial or sexually explicit e-mail is guilty of a class-B misdemeanor[103] and remains liable to civil action.[104] All

[98] See s 17529.4(b) of the California and Business Professions Code and s 3-805-1(b) (6)(i) of the Maryland Criminal Law Code.

[99] See s 17529.4(c) (1) and (2) of the California Business Professions Code.

[100] See s 4-88-607(a)-(c) of the Arkansas Code; and s 13.36-104 of the Utah Statutes.

[101] See s 4-88-607(b) of the Arkansas Code and s 776.7 of the Oklahoma Statutes.

[102] See s 37-24-6(13) of the South Dakota Codified Laws and s 46.005 of the Texas Statutes.

[103] See s 4-88-605 of the Arkansas Code; s 46.005 of the Texas Statutes; and s 445.2507(7) of the Michigan Compiled Statutes. Misdemeanors are classifications for less serious criminal offences. Every state in the USA has a system for classifying criminal offences. There are three

remedies, penalties, and authority are available to the Attorneys-General in those states when the question of enforcement arises.[105]

(b) Civil action

An action may be brought by any person who has received unsolicited commercial e-mail or unsolicited sexually explicit e-mail which violates the legislative provisions of the state in which the actual damages are to be recovered.[106] Each recipient or e-mail service provider shall be awarded costs and reasonable attorneys' fees.[107]

Some states require that whoever violates the provisions above shall be liable for damages to the recipient of an unsolicited commercial e-mail message in the amount of one hundred dollars ($ 100) for each violation, as well as reasonable attorneys' fees and costs.[108] The damages also extend to the injury that the recipient (and not the e-mail service provider or its property) might have sustained arising out of the transmission of unsolicited bulk mail.[109]

6.2.2.7 Commentary and conclusion

The prohibitions listed above apply to any person doing business in a particular state and to any person who transmits commercial e-mail messages from a computer

classes of misdemeanor namely: class A-C with "class A" being the highest level and "class C" the lowest; "class B" misdemeanors are punished by between 90-180 days in a county jail. See FreeAdvice 'What are class A, B, and C misdemeanors' http://criminal–law.freeadvice.com/criminal-law/white_collar_crimes/criminal-misdemeanor-clases.html (date of use: 30 December 2015).

[104] See s 4-88-605(a)(b) of the Arkansas Code and s 13-36-104 of the Utah Code.

[105] See s 4-88-607(a)-(c) of the Arkansas Code; and ibid the Utah Code.

[106] Damages include: (a) ten dollars per unsolicited commercial e-mail or unsolicited sexually explicit e-mail sent to a previously opted-out e-mail address, or transmitted through the e-mail service provider, or otherwise sent in violation of the provisions of a particular Act; and (b) US $25 000 per day while the violation continues. See s 4-88-606 of the Arkansas Code and section 47-16-2501(i)(2) of the Tennessee Code.

[107] See s 4-88-606(2) of the Arkansas Code; s 44-1372.02 of the Arizona Revised Statutes; and s 53-452(a) and (b) of the General Statutes of Connecticut.

[108] See s 3-805.1(c) of the Maryland Criminal Law Code; also s 6-47-2(h) of the Rhode Island General Laws Title 6 Commercial Law Chapter 7 Internet Access and Advertising by Facsimile (added in 1999).

[109] See s 47-16-2501(i)(2) of the Tennessee Statutes. In other states the civil penalty imposed are for the first violation not exceeding US $500; for a second violation not exceeding US $2 500; and for the third and subsequent violations, not exceeding US $5 000; also s 16-9-105 (b) the Official Code of Georgia; and s 40-12-403(a) of the Wyoming Statutes.

located in that state.[110] They further apply to an e-mail address which the sender knows, or has reason to know, is held by a resident of that state, and to an interactive computer service with equipment or its principal place of business in that state.[111]

Almost all of the anti-spam legislation considered above meets the requirements for strong legislation which include: definition(s) of what constitutes spam; mechanisms in place in order to regulate spam; and other requirements for the sending of unsolicited messages such as labelling, falsification of headers, and prohibiting harvesting or selling e-mail lists. Penalties are prescribed for non-compliance with the provisions of these laws. However, while state laws have been successful in protecting consumers locally, some are of the view that the same "are ill-equipped to deal with the issue of spam originating from beyond each state's boundaries".[112]

Others have noted that the anti-spam laws above "may stifle the growth of online commerce by hampering the flow of otherwise accurate information from emerging Internet merchants to consumers".[113] Also that, instead of eliminating spam, the statutes are seen to be placing unnecessary limitations on legitimate Internet marketers and denying consumers the choices a rich Internet marketplace would provide.[114] While most of these state laws have been effective in regulating spam, the enactment of the federal law has had the effect of pre-empting many of their provisions.[115] Despite the pre-emptive nature of the federal law, certain provisions in state laws can also be identified in the federal law as pointed out below.

[110] See s 44-1372.01(E); also s 44-1372.04 of the Arizona Revised Statutes, which deals with instances in which the Act does not apply; and s 39-14-604(b) of the Tennessee Code.

[111] Ibid.

[112] See Amaditz (1999) 4 *Virginia Journal of Law and Technology* http://www.vjolt.net/vol4/issue/home.art4.html (date of use: 30 December 2015).

[113] Kendrick supra n 10 575.

[114] Ibid 576.

[115] The state of North Dakota had a provision in its statute that "the Governor shall certify to the legislative council the effective date of any federal legislation that pre-empts state regulation of false, misleading, or unsolicited commercial e-mail messages. That Act became ineffective upon the effective date contained in the certification of federal legislation that pre-empts state regulation of false, misleading or unsolicited commercial e-mail message". See s 2 of the North Dakota Statutes and s 325M.09(11) of the Minnesota Statutes 2002 Ch 395 Senate file no 2908 (2002) (introduced 11 February 2002 approved 20 May 2002).

6.3 Anti-spam legislation at federal level

6.3.1 Background

The Controlling the Assault of Non-Solicited Pornography and Marketing Act[116] is the USA's federal anti-spam law. It was adopted in 2003 and came into operation in January 2004.[117] Section 2 of the CAN-SPAM Act highlights congressional findings and policy which include among others: the importance and convenience of low cost e-mail relied on by its citizens on a daily basis;[118] that convenience and efficiency is under threat from the extremely rapid growth in the volume of unsolicited commercial e-mail;[119] that some messages contain material that recipients might consider vulgar or pornographic; and that many senders of such mail intentionally disguise the source of the mail to include misleading information in the message subject lines in the hope of inducing recipients to view the messages;[120] and that while some senders of commercial e-mail provide simple and reliable ways for recipients to reject receipt of their e-mails in the future, other senders provide no such (opt-out) mechanism, or refuse to honour such requests.[121]

Senders[122] have been known to use computer programs to gather large numbers of e-mail addresses on an automated basis from Internet web sites or online services where users post their addresses in order to make full use of the web site(s) or service(s).[123] It was also pointed out that the problems associated with the rapid growth and abuse of unsolicited commercial e-mail cannot be solved by federal

[116] Hereafter 'the CAN-SPAM Act'.

[117] See s 16 of the CAN-SPAM Act. Former USA President Bush signed this Act into law. The background statement to his presidential action on the day the law was passed noted the following: "that spam is a problem for Americans; that the law provides a well-balanced approach that will help to address some of the harmful impacts of spam; the law builds upon the Administration's efforts to empower consumers with choices in the technology field; the law strengthens a cornerstone of the administrations agenda to help protect children against pornography; and the Administration supports the law's tools to help deter the harmful effects of deceptive and misleading spam". See The White House 'Fact sheet: President Bush signs anti-spam law' http://www.whitehouse.gov/news/releases/ 2003/12/print/20031216-4.html (date of use: 30 December 2015).

[118] See s 2 (a)(1) of the CAN-SPAM Act.

[119] Id s 2(a)(3) and (6).

[120] Id s 2(a)(5), (7) and (9).

[121] Id s 2(a)(9).

[122] Id s 3(16)(A) which defines the term "sender" as "a person who initiates such a message and whose product, service, or Internet web site is advertised or promoted by the message".

[123] Id s 2(a)(10).

legislation alone.[124] New technological approaches and cooperation between countries will also play a significant role in limiting (or eliminating) spam.[125] Section 3(2)(A) of the CAN-SPAM Act notes that this Act was enacted "to regulate interstate commerce by imposing limitations and penalties on the transmission of unsolicited commercial e-mail via the Internet".[126] The purpose of the CAN-SPAM Act is to cover "commercial e-mail messages whose primary purpose is the commercial advertisement or promotion of commercial product or services including content on an Internet web site operated for a commercial purpose".[127]

The CAN-SPAM Act establishes requirements that must be met by those who send commercial e-mail and spells out penalties for senders and companies whose products are advertised in spam if they violate the law.[128]

6.3.2 Anti-spam provisions under CAN-SPAM Act of 2003

6.3.2.1 Definitions

The term "commercial e-mail message" is defined as "any e-mail message the primary purpose of which is the commercial advertisement or promotion of a commercial product or service (including content on an Internet web site operated for a commercial purpose)".[129] This term does not include "transactional" or "relational messages".[130] The federal law, like most of the state laws above, defines spam from a content (commercial) perspective and not necessarily in terms of volume or bulk.
The term "e-mail address" means "a destination, commonly expressed as a string of characters, consisting of a unique user name or mailbox (commonly referred to as

[124] Id s 2(a)(12).

[125] Ibid.

[126] See the Preamble to the CAN-SPAM Act 2003; also Fagan (2004) 33/10 *The Colorado Lawyer* 61 ff, for a general discussion on the CAN-SPAM Act; Lavergne (2005) 1/3 *NYU Journal of Law & Business* 861 ff; and Baxter (2004) 8/1 *NYU Journal of Legislation and Public Policy* 165-9.

[127] Section 3(2)(A) of the CAN-SPAM Act.

[128] Ibid s 4-6. These requirements are discussed in detail below.

[129] Ibid s 3(2)(A). This definition is in line with the definition of unsolicited commercial communications at state level. Also see Marks (2004) 54/3 *Case Western Reserve Law* 943 and Alongi (2004) 46/2 *Arizona Law Review* 288.

[130] See s 3(2)(B)) of the CAN-SPAM Act. A "transactional" or "relational message" means "an e-mail message whose primary purpose is to facilitate, complete, or confirm a commercial transaction that the recipient has previously agreed to enter into with the sender; or to provide warranty information, product recall information, or safety or security information with respect to a commercial product or service used or purchased by the recipient".

the local part) and a reference to an Internet domain (commonly referred to as the domain part), whether or not displayed to which an e-mail message can be sent or delivered".[131] On the other hand, the term "e-mail message" is defined as "a message sent to a unique e-mail address".[132]

6.3.2.2 Mechanism to regulate spam: Opt-out mechanism

The CAN-SPAM Act, like most of the state laws before it, has adopted the opt-out mechanism which allows spammers to send unsolicited messages provided that each message complies with the provisions of the Act. The following are the requirements for sending unsolicited e-mail messages.

(a) Inclusion of identifier, opt-out, and physical address in commercial e-mail

The CAN-SPAM Act makes it unlawful for any person to initiate[133] transmission to a protected computer[134] unless the message provides a clear and conspicuous identification that it is an advertisement or solicitation.[135] It must also provide for a clear and conspicuous notice of the opportunity to decline to receive further commercial e-mail message from the sender.[136] The opt-out address should also include a valid physical postal address for the sender.[137] This provision does not apply if the recipient has given prior consent[138] to receive a commercial e-mail message.

[131] Id s 3(5).

[132] Id s 3(6). Other definitions are defined as the discussion continues below.

[133] The term "initiate" is defined in s 3(9) of the CAN-SPAM Act as meaning "to originate or transmit such message or to procure the origination or transmission of such message, but shall not include actions that constitute routine conveyance of such message".

[134] Id s 3(13). The term "protected computer" has a meaning given that in terms of s 1030(e)(2)(B) of Title 18 of the United States Code (this section deals with fraud).

[135] Id s 5(a)(5)(i).

[136] Id s 5(a)(5)(ii).

[137] Id s 5(a)(5)(iii).

[138] Id s 3(1)(A) and (B) which defines the term "affirmative consent" as "the recipient expressly consented to receive the message either in response to a clear and conspicuous request for such consent or at the recipient's own initiative; and if the message is from a party other than the party which the recipient communicated such consent, the recipient was given clear and conspicuous notice at the time the consent was communicated that the recipient's electronic mail address could be transferred to such other party for the purpose of initiating commercial electronic mail message". Compare this definition with that in n 44 above.

(b) Inclusion of return address or comparable mechanism in commercial e-mail

In addition to the opt-out mechanism, the CAN-SPAM Act requires that an address be included in a commercial e-mail message that is sent which clearly and conspicuously display a functional return e-mail message or other Internet-based mechanism.[139] A recipient must be able to use this functional return e-mail address to submit, in a manner specified, a reply e-mail message or other form of Internet-based communication requesting not to receive future commercial e-mail messages from the sender at the e-mail address where the message was received.[140] The mechanism must be able to receive such requests or communications not less than 30 days after the transmission of the original message.[141]

The recipient should be provided with a list or menu from which he or she may choose the specific types of commercial e-mail message they wish or do not wish to receive from the sender.[142] However, the list or menu must include an option under which the recipient may choose not to receive any commercial e-mail messages from the sender.[143] Should the return e-mail address or other mechanism temporarily be unable to process requests due to some technical problems beyond the control of the sender, that sender will not be held accountable for failing to comply with the requirements of the CAN-SPAM Act.[144] However, the sender should make sure that the problem is corrected within a reasonable time.[145]

(c) Prohibition of transmission of commercial e-mail after objection

If a recipient using a mechanism provided in the Act requests not to receive some or any commercial e-mail messages from a sender, it is unlawful:[146]

[139] Ibid s 5(a)(3)(A)(i-ii).

[140] Ibid.

[141] Ibid.

[142] Id s 5(3)(B).

[143] Id s 5(a)(3)(B).

[144] Id s 5(a)(3)(C).

[145] Ibid.

[146] Id s 5(a)(4)(A).

> (1) For the sender to initiate the transmission to the recipient, more than 10 business days after the recipient of such request, of a commercial e-mail message that falls within the scope of the request;[147]
> (2) For any person acting on behalf of the sender to initiate the transmission to the recipient, more than 10 business days after the receipt, of a commercial e-mail message with actual knowledge, or knowledge fairly implied on the basis of objective circumstances, that such message falls within the scope of the request;[148]
> (3) For any person acting on behalf of the sender to assist in initiating the transmission to the recipient, through the provision or selection of addresses to which the message will be sent, of a commercial e-mail message with actual knowledge or knowledge fairly implied on the basis of the objective circumstances, that such message would violate clause (i) and (ii); or[149]
> (4) For the sender or any other person who knows that the recipient has made such a request, to sell, lease, exchange, or otherwise transfer or release the e-mail address of the recipient (including through any transaction or other transfer involving mailing lists bearing the e-mail address of the recipient) for any purpose other than compliance with this Act or other provision of law.[150]

Kikuchi opines that “the opt-out system is burdensome because both the sender and those acting on his or her behalf must comply with opt-out requests, which will drastically affect joint-marketing relationships because multiple parties must communicate with each other very efficiently if they hope to comply within the required ten-day deadline”.[151] The opt-out system is therefore viewed as ineffective, inefficient, and burdensome because for that system to work it must be fully operational and the e-mail address provided for such opt-out purposes must be accurate in order for the sender to process that request.[152]

6.3.2.3 Requirements for transmission of e-mail messages

Section 5 of the CAN-SPAM Act provides the following requirements for transmission of commercial electronic messages in order to protect recipients[153] who use commercial e-mail.

[147] Id s 5(a)(4)(A)(i).

[148] Id s 5(a)(4)(A)(ii).

[149] Id s 5(a)(4)(A)(iii).

[150] Id s 5(a)(4)(A)(iv).

[151] Kikuchi (2004) 10/2 *BU J Sci & Tech L* 285. Kikuchi notes that “this will likely lead to the creation of massive lists of opted-out addresses that will need to be passed down a long line of vendors in order to comply, creating a huge burden on businesses which endeavor to comply with the Act”.

[152] On the other hand, by requesting to opt-out the user might be confirming that they are alive thus getting more spam e-mails from others. Id 285-6; and Lorentz (2011) 30/3 *Review of Litigation* 589-92 where the author discusses the major problems inherent in the CAN-SPAM Act, namely: the loophole for list owners; and clicking on potential virus links.

[153] Section 3(14) of the CAN-SPAM Act defines the term “recipient” as meaning “an authorised user of the e-mail address to which the message was sent or delivered. If a recipient of a commercial e-mail message has one or more e-mail addresses in addition to the address to which the message was sent or delivered, the recipient shall be treated as a separate recipient

(a) Prohibition of false or misleading transmission information

Section 5(a) (1) of the CAN-SPAM Act prohibits the transmission of a commercial e-mail message that contains header information[154] that is materially false or materially misleading.[155] The CAN-SPAM Act considers a "header information" to be "materially misleading if it fails to identify accurately a protected computer used to initiate the message because the person initiating the message knowingly used another protected computer to relay or retransmit the message for purposes of disguising its origin".[156] According to Fingerman, the aim of this provision is to force spammers to identify themselves in their mailings.[157] The CAN-SPAM Act prohibits any person transmitting false or misleading information by e-mail knowingly.[158] This section also prohibits promotions made by a business in the knowledge that the header information is misleading or false, or where it should have known this and reasonable steps should have been taken to prevent such transmission.[159]

(b) Prohibition of deceptive subject headings

The CAN-SPAM Act prohibits the transmission of commercial e-mail messages by persons who have actual knowledge, or knowledge fairly implied that a subject heading of the message is likely to mislead recipients as to the contents or subject

with respect to each address". Compare this with definition of recipient under state laws in n 52 above.

[154] Section 3(8) of the CAN-SPAM Act defines the term "header information" as "a source, destination, and routing information attached to an e-mail message, including the originating domain name and originating e-mail address, and any other information that appears in the line identifying, or purporting to identify, a person initiating the message". Compare with definition of header information under state laws n 74 above.

[155] See s 5(a)(1) of the CAN-SPAM Act. The term "materially" for purposes of this provision when used with respect to false or misleading header information, "includes the alteration or concealment of header information in a manner that would impair the ability of an Internet access service processing the message on behalf of a recipient, a person alleging a violation of this section, or a law enforcement agency to identify, locate, or respond to a person who initiated the e-mail message or to investigate the alleged violation, or the ability of a recipient of the message to respond to a person who initiated the electronic message" (see s 5(a)(6) of the CAN-SPAM Act). Compare state definition of "materially falsified" in n 69 above.

[156] See s 5(a)(1)(C) of the CAN-SPAM Act.

[157] See Fingerman (2004) 7/8 *Journal of Internet law* 1-14 http://www.danfingerman.com/papers/CAN-SPAM.doc (date of use: 30 December 2015). Fingerman points out that "a header has three parts: address information (which controls where the e-mail is delivered); origin information (which documents where the message originated); and routing data (which documents the intermediary mail server that handled the message as it traversed the Internet)".

[158] See s 6 of the CAN SPAM Act.

[159] Id s 6(a).

matter of the message.[160] In 2004 the Federal Trade Commission announced the first cases that contained deceptive messages contravening the provisions of the CAN-SPAM Act.[161]

Federal Trade Commission v Phoenix Avatar LLC

The facts in *Federal Trade Commission v Phoenix Avatar, LLC*[162] were as follows: Phoenix Avatar, a company based in Detroit, sent illegal spam messages selling false diet patches. Consumers who wished to buy the products clicked on a hyperlink in the message and were connected to one of the defendant's web sites.[163] It was alleged that the defendant earned $100 000 per month from product sales. It was further alleged that the claims made for these diet patches were false and that the patches, which sold for $59.95 each, had no effect at all.[164] The defendant obscured (spoofed) their identities by using third party e-mail addresses in the 'reply-to' or 'from' fields of their spam e-mails.[165] When the spam message was undelivered it bounced back to unwitting third parties who were themselves incorrectly labelled as spammers.[166] The defendants were ordered to pay monetary relief in the amount of $230 000 in favour of the Commission as equitable monetary restitution for consumer injury relief.[167]

FTC v Global Web Promotions Pty Ltd

[160] Id s 5(a)(2).

[161] Federal Trade Commission 'FTC announces first CAN-SPAM cases: two operations generated nearly one million complaints to agency' http://www.ftc.gov/news-events/press-releases/2004/04/ftc-announces-first-can-spam-act-cases (date of use: 30 December 2015).

[162] See *Federal Trade Commission v Phoenix Avatar, LLC (trading as Avatar Nutrition)* case no 04C 2897 (2004) 1-24 http://www.ftc.gov/sites/default/files/documents/cases/2005/03/050331stip0423084.pdf (date of use: 30 December 2015). Hereafter '*Phoenix Avatar* case'.

[163] See Consumer Affairs 'Feds nab two big spammers: defendants have sent millions of deceptive messages, investigators say' http://www.consumeraffairs.com/news04/ can_spam.html (date of use: 30 December 2015).

[164] Ibid.

[165] See Federal Trade Commission 'FTC announces first CAN-SPAM cases: two operations generated nearly one million complaints to agency' supra n 161.

[166] Ibid.

[167] See *Phoenix Avatar case* supra n 162 9 for a stipulated order for the permanent injunction and final judgment.

In *FTC v Global Web Promotions Pty Ltd*[168] an Australian company was alleged to have been responsible for massive amounts of spam in the United States. This company advertised its diet patch – similar to that offered in *Phoenix Avatar* – which sold for $ 80.90. They also sold human growth hormone (HGH) for $ 74.95.[169] The company further claimed its HGH and natural HGH could maintain the appearance and current biological age of the user for the next ten to twenty years.[170] The FTC introduced as evidence thousands of spoofed e-mails sent to victims which included AOL, Microsoft software, and other companies.[171]

The court found that the defendants had initiated transmission to protected computers of commercial e-mail messages that contained materially false and misleading header information in violation of the CAN-SPAM Act.[172] The court found that a monetary judgment against the defendants for an amount of $ 490 280 was proper for consumer injury resulting from the sale of diet patches and HGH products.[173] The court also found that the total ill-gotten gains received by the defendants in violation of the Act was $ 1 700 982.74.[174]

Federal Trade Commission v Spear Systems Inc et al

In *Federal Trade Commission v Spear Systems Inc et al* [175] the defendants were found to be in violation of the CAN-SPAM Act for their deceptive acts or practices in connection with the sale of *hoodia gordinii* and HGH products, and also the initiation of commercial e-mail messages in violation of the CAN-SPAM Act.[176] The FTC had filed a lawsuit against the defendants who were allegedly using other web sites to sell fake weight-loss supplements.[177] The court found that the defendants had

[168] *FTC v Global Web Promotions Pty Ltd* case no 04C 3022 (2005) 1-23 http://www.ftc.gov/sites/default/files/documents/cases/2005/09/050920defjudg0423086.pdf (date of use: 30 December 2015). Hereafter '*Global Web Promotions* case'.

[169] Id 2.

[170] Ibid.

[171] Ibid.

[172] See s 5(a)(1) and 5(a)(5)(A) of the CAN-SPAM Act; and id 6.

[173] Id 2-7.

[174] Id 7.

[175] See *Federal Trade Commission v Spear Systems Inc* case no 07 c 5597 (2009) 1-22 http://www.ftc.gov/sites/default/files/documents/cases/2009/07/090702xavierjudgeorder.pdf (date of use: 30 December 2015). Hereafter '*Spear Systems* case'.

[176] Id 3.

[177] Id 4.

initiated the transmission of commercial e-mail messages containing header information that was materially false or misleading in violation of the CAN-SPAM Act to protected computers.[178] The court considered it proper in this case to enter equitable monetary relief against defendants for consumer injury and ill-gotten gains in the amount of $ 3 701 088.33.[179]

Other cases include a spammer who was ordered to stop selling fake weight-loss and anti-aging products, and to also pay more than $ 2.5 million.[180] And another case included a 'spam gang' ordered to pay $ 15.15 million for deceptively marketing male enhancement pills, prescription drugs, and weight-loss pills.[181]

US v Twombly

In *US v Twombly*[182] the defendant (Twombly) leased servers using an alias so as to send large numbers of e-mail messages.[183] The defendant allegedly sent approximately one million spam e-mail messages within two hours after he had been provided with logon credentials by Biznesshosting Inc.[184] This was followed by a further 1.5 million e-mail messages days after the first batch was sent out.[185] It was alleged that the web site was falsely registered under the name of a non-existent business, and that the message routing information and "from" lines had been falsified so preventing recipients, ISPs, and law enforcement agencies from identifying, locating, or responding to senders.

[178] Id s 5(a)(1) and 5(a)(2).

[179] Id 6.

[180] See *Federal Trade Commission v Sili Neutraceuticals LLC* case no 07 C 4541 (2008) 1-20 http://www.ftc.gov/sites/default/files/documents/cases/2008/02/080123silidefaultjdgmnt.pdf (date of use: 30 December 2015); Federal Trade Commission 'Judge agrees with FTC, orders spammers to pay more than $2.5 million and stop selling bogus weight-loss and anti-aging products' http://www.ftc.gov/news-events/press-releases/2008/02/judge-agrees-ftc-orders-spammers-pay-mpre-25-million-and-stop (date of use: 30 December 2015).

[181] See *Federal Trade Commission v Lance Thomas Atkins* case no 08CV5666 (2009) http://www.ftc.gov/sites/default/files/documents/cases/2009/11/091130atkinsjudgement.pdf (date of use: 30 December 2015).

[182] See *US v Twombly* 475 F Supp 2nd 1019 (SD Cal 2007) 1-11 https://casetext.com/case/us-v-twombly-2 (date of use: 30 December 2015). Hereafter '*Twombly* case'.

[183] Id 2.

[184] Ibid.

[185] Ibid.

The defendants filed a motion seeking, among other things, dismissal of their indictment on the basis that the statute under which they had been charged – section 1037(a)(3) and (4) of the 18 United States Code (USC) – was unconstitutionally vague.[186] Further, the defendants argued that a header does not necessarily identify the sender, and that a lay person has little or no ability to trace the sender's location based on the address.[187] They also argued that because the lay person's ability to identify senders is inherently impaired, the statute is meaningless.[188] The court noted that even if recipients could not identify senders from header information, the defendant had not shown that this applied equally to all users.[189] It therefore found that the section was not unconstitutional, vague, or overboard and denied the defendants' motion to dismiss the indictments based on the section.[190]

US v Kilbride

The provisions of the CAN-SPAM Act were again challenged as being unconstitutionally vague, this time in the United States Court of Appeals. In *US v Kilbride*[191] the facts were briefly that the defendants began their bulk e-mail advertising business in 2003 operating through an American corporation using servers in the state of Arizona.[192] They then moved their operations overseas, running them through Ganymede Marketing, a Mauritian company, using servers located in the Netherlands.[193] The advertisements appearing in the defendants e-mails included sexually explicit images, two of which formed the basis for their conviction on obscenity charges. The defendant's employees used fictitious information in headers and nonsensical domain names that matched generic user names to generate a series of different non-functional e-mail addresses to which to

[186] Section 1037(a)(3) and (4) deals with materially falsifying header information in multiple commercial e-mail messages and intentionally initiating the transmission of those e-mail messages.

[187] *Twombly* case supra n 182 2 and 5.

[188] Ibid.

[189] Ibid.

[190] Id 7.

[191] See *US v Kilbride* 584 F 3d 1240 (9th Cir 2009) 1-19 http://www.nyls.edu/wp-content/uploads/sites/141/2013/08/584-F.3d-1240-US-v.-Kilbride.pdf (date of use: 30 December 2015). Hereafter '*Kilbride* case'.

[192] Id 1-3.

[193] Ibid.

send their bulk e-mail advertisements.[194] These were placed in the field "from" of the headers so falsifying information appearing in the registration of the domain names used. Nine counts were brought against the defendants including violation of section 1037(a)(3) and (4) of 18 USC.[195] The defendants were convicted on all counts following a three-week jury trial.[196] The court held that the criminal prohibitions in section 1037(a)(3) and (4) 18 USC were not unconstitutionally vague.[197] The defendants were sentenced to 63 and 78 months in prison for misdemeanours, sending fictitious information in the headers of bulk e-mails, and creating nonsensical domain names and matching them with generic user names to generate a series of different e-mail addresses.[198]

(c) Aggravated violations relating to commercial e-mail

The CAN-SPAM Act prohibits any person "to initiate the transmission of a commercial e-mail message, or to assist in the origination of such messages, through the provision or selection of addresses to which the message will be transmitted, if that person had actual knowledge or knowledge fairly implied on the basis of objective circumstances which includes address harvesting and dictionary attack".[199]

Address harvesting

Section 5(b)(A)(i) of the CAN-SPAM Act makes provision for harvesting of e-mail addresses of recipients that were obtained using an automated means from an Internet web site or proprietary online service operated by another person, (including web site or online service). This also covers a notice stating that "operators of such web sites or online service will not give, sell, or otherwise transfer addresses maintained by the web site or online service to any other party for the purpose of

[194] Ibid.

[195] This section deals with materially falsifying header information in multiple commercial electronic mail messages and intentionally initiating the transmission of such messages. See Cornell University Law School '18 U.S s 1037 – Fraud and related activity in connection with electronic mail' https://www.law.cornell.edu/uscode/text/18/1037 (date of use: 30 December 2015).

[196] See *Kilbride* case supra n 191 3.

[197] Id 3 and 13-19.

[198] Id 3-4.

[199] See s 5(b)(1)(A) of the CAN-SPAM Act.

initiating or enabling others to initiate e-mail message(s)".[200] Kikuchi notes that this provision contains a weak prohibition on harvesting, contingent on violations of other provisions of the Act.[201] That author further notes that users are fearful because they will not be able to make full use of web sites and Internet services if their addresses are constantly being harvested by spammers.[202] They also note that this provision does not entirely prohibit the alphanumeric automated creation of addresses and harvesting and also does not require user consent.[203]

Dictionary attacks

The CAN-SPAM Act also makes it unlawful for any person to obtain the e-mail address of a recipient using an automated process that generates possible mail addresses by combining names, letters, or numbers into numerous permutations.[204]

Automated creation of multiple e-mail accounts

CAN-SPAM Act also outlaws the use by any person of scripts or other automated means to register for multiple e-mail accounts or online user accounts from which to transmit to a protected computer, or enable another person to transmit to a protected computer, a commercial e-mail message.[205] This includes the relay or re-transmission through unauthorised access.[206]

(d) Placing warning labels on commercial e-mail containing sexually-oriented material

[200] Id s 5(b)(A)(i).
[201] Kikuchi supra n 151 286.
[202] Ibid.
[203] Id 287.
[204] See s (5)(b)(1)(A)(ii) of the CAN-SPAM Act. Compare with para 6.2.2.5 above on the issue of address harvesting at state level.
[205] See s 5(b)(2).
[206] Id s 5(b)(3). This section makes it unlawful for any person knowingly to relay or re-transmit commercial e-mail messages that are unlawful in terms of the CAN-SPAM Act, from a protected computer or computer network that he or she has accessed without authorisation.

Section 5(d) of the CAN-SPAM Act requires that warning labels be placed on any commercial e-mail message that includes sexually-oriented material.[207] This provision makes it unlawful for any person who fails to include in the subject heading for the e-mail message, the prescribed marks or notices,[208] or fails to provide that the matter in the message that is initially viewable by the recipient, when the message is opened by any recipient and absent of any further actions by the recipient including:[209] to the extent required or authorized pursuant to paragraph (2) any such marks or notices;[210] the information required to be included in the message pursuant to subsection (a)(5);[211] and instructions on how to access, or a mechanism to access the sexually-oriented material.[212]

This section does not apply to the transmission of an e-mail message if the recipient has given prior consent to receive the message.[213] Those who knowingly violate this provision shall be fined or sentenced to imprisonment for not more than five years, or to both.[214] The CAN-SPAM Act also provides that not later than 120 days after the date of the enactment of the Act that clearly identifiable marks or notices should be included in or associated with commercial e-mail containing sexually-oriented material, in order to inform the recipient of that fact and to facilitate the filtering of such e-mail.[215] The Commission was tasked with the publication of the marks or notices prescribed in the Federal Register and to provide notice to the public.[216]

[207] The term "sexually explicit material" is defined as "any material that depicts sexually explicit conduct unless the depiction constitutes a small and insignificant part of the whole, the remainder of which is not primarily devoted to sexual matters". See id s 5(d) (4).

[208] Id s 5(d)(1)(A).

[209] Id s 5(d)(1)(B).

[210] Id s 5(d)(1)(B)(i).

[211] Id s 5(d)(1)(B)(ii).

[212] Id s 5(d)(1)(B)(iii). Compare with para 6.2.2.3 above where this issue is dealt with at state level.

[213] Id s 5(d)(2).

[214] Id s 5(d)(5).

[215] Id s 5(d)(3).

[216] Ibid. The Federal Register outlining the requirements to place warning labels on e-mail that contains sexually oriented material was published on 29 January 2004, and the following requirements were outlined: "that any person who initiates to a protected computer, the transmission of a commercial e-mail message that includes sexually oriented material must: Include in the subject heading for that e-mail message the phrase "SEXUALLY-EXPLICIT-CONTENT" in capital letters as the first twenty seven (27) characters at the beginning of the subject line; provide that the content in the message initially viewable by the recipient when the message is opened include the following phrase "SEXUALLY-EXPLICIT-CONTENT" in a clear and conspicuous manner; clear and conspicuous identification that the message is an advertisement or solicitation; clear and conspicuous notice of the opportunity of a recipient to decline to receive further commercial electronic mail messages from the sender; and a functioning return electronic mail address or other Internet-based mechanism clearly and

Eighteen months after the date of enactment of the CAN-SPAM Act a report was compiled setting out a plan requiring commercial e-mail to be identifiable from its subject line.[217] The CAN-SPAM Act also deals with the prohibition of predatory and abusive commercial e-mail the transmission of which is regarded as a misdemeanour and attracts criminal liability for certain spam-related activities.[218]

6.3.2.4 Enforcement of the Act

(a) Background

The CAN-SPAM Act provides general enforcement rules which are to be applied by the Commission as if the violation of the Act amounted to unfair or deceptive acts.[219] Enforcement can also be undertaken by certain agencies as provided for in the Act.[220]

(b) The Commission

In terms of the CAN-SPAM Act the Commission shall "prevent any person from violating the Act in the same manner, by the same means, and with the same

conspicuously displayed". See Federal Register 'Requirements to place warning labels on commercial electronic mail that contains sexually oriented material' v 69 n 19 (29 January 2004) 1-5 http://www.uspto.gov/sites/ default/files/web/offices/com/sol/notices/69fr4269.pdf (date of use 6 January 2016); also s 316.4 16 Code of Federal Regulation (CFR) Part 316 Title 16 Commercial Practices where the above phrase "sexually explicit content" was amended to: SEXUALLY-EXPLICIT which now comprise of 17 characters including the (-) between the words https://www.law.cornell.edu/cfr/text/16/316.4 (date of use: 6 January 2016).

[217] See s 11 (1)(B) of the CAN-SPAM Act. See Platt Majoras D et al 'Subject line labelling as a weapon against spam: A CAN-SPAM Act Report to Congress' (June 2005) 1-46 https://www.ftc.gov/sites/default/files/documents/reports/subject-line-labeling-weapon-against-spam-can-spam-reprt-congress/050616canspamrpt.pdf (date of use: 6 January 2016). This report outlined the following as recommendations against subject-line labelling which included: (a) a mandatory subject line labelling is likely not an effective tool for ISPs to block and filter spam; (b) there are technological concerns with subject labelling requirements; and (c) mandatory subject line labelling would not strengthen anti-spam law enforcement (at 10-18).

[218] See s 4 of the CAN-Spam Act.

[219] These includes practice prescribed under s 18(a)(1)(B) of the Federal Trade Commission (FTC); also Federal Trade Commission 15 USC. 57a (a)(1)(B) (this section deals with unfair or deceptive acts or practices https://www.law.cornell.edu/uscode/text/15/57a (date of use: 30 December 2015); also s 7(a) of the CAN-SPAM Act.

[220] Id s 7(b) of the CAN-SPAM Act. These include, among others, agencies regulated by the following legislation: s 8 of the Federal Deposit Insurance Act (12 USC 1818); and Federal Credit Union Act (12 USC 1751).

jurisdiction, powers, and duties as if all applicable terms and provisions of the Federal Trade Commission Act were incorporated into and made part of the Act".[221]

(c) The State

Civil action

In any case in which a state Attorney-General or an official or agency of a state has reason to believe that an interest of the residents of that state have been or are threatened or adversely affected by any person who has violated some provisions of the CAN-SPAM Act,[222] that Attorney-General, official, or agency may bring a civil action on behalf of the residents of the state in a district court of the United States having appropriate jurisdiction[223] The availability of injunctive relief without a showing of knowledge is also covered in the CAN-SPAM Act.[224]

Statutory damages

Regarding aggravated damages, the court may increase the damage awarded to an amount equal to not more than three times the amount otherwise available under section 7(f)(1)(B)(ii) if it finds that the defendant committed the violation willfully and knowingly,[225] or that his or her unlawful activity included one or more of the aggravated violations listed in section 5(b).[226] In assessing damages under this provision the court may consider whether the defendant has established and implemented with due care, commercially reasonable practices and procedures

[221] See the Federal Trade Commission Act (15 USC 41); and s 7(d) of the CAN-SPAM Act.

[222] These include: s 5(a)(1) and (2) which deals with the prohibition of false or misleading transmission of information and the prohibition of deceptive subject headings.

[223] This can be done to enjoin further violation of s 5 of the CAN-SPAM Act by the defendant; or (b) to obtain damages on behalf of residents, in an amount equal to the greater of: the actual amount monetary loss suffered by such residents; or the amount determined under para 3 of this section. See s 7(f)(1)(a) and (b) of the CAN-SPAM Act.

[224] This will apply to the following sections: Id s 5(a)(1)(C) which deals with header information that is considered materially misleading; s 5(a)(2) dealing with the prohibition of deceptive subject headings; s 5(a)(4)(A) which covers the prohibition of transmission of commercial e-mail after objection; s 5(b)(1)(A) on aggravated violations relating to commercial e-mail in particular address harvesting; s 5(b)(3) which covers the relay or transmission through unauthorised access; and s 7(f)(2).

[225] Id 7(f)(3)(C)(i).

[226] Id s 7(f)(3)(C) (ii).

designed effectively to prevent such violations.[227] It may further consider whether the violations occurred despite commercially reasonable efforts to maintain compliance with the practices and procedures to which reference is made in clause (i).[228] In the case of any successful action, the court may, in its discretion, award the costs of the action and reasonable attorney fees to the state.[229]

(d) Action by provider of an Internet access service

Where an Internet Access Service Provider (IASP)[230] is adversely affected by a violation of the sections of the Act dealing with the following: deceptive headings; non-inclusion of a return address; prohibition of transmission after objection; and non-inclusion of identifier opt-out mechanism,[231] that IASP may bring a civil action in any district court of the United States with jurisdiction over the defendant.[232]

The CAN-SPAM Act also deals with the determination of the amounts to be paid for unlawful messages transmitted or attempted to be transmitted over the facilities of the IASP, or messages transmitted or attempted to be transmitted to an e-mail address obtained from the IASP in violation of the Act.[233] The court may increase a damage award to an amount equal to not more than three times the amount otherwise available under this paragraph[234] if it finds that the defendant committed

[227] Id s 7(f)(D)(i).

[228] Id s 7(f)(3)(D)(ii).

[229] Id s 7(f)(3)(4) s 7(f)(4).

[230] Id s 3(11) which defines the term “Internet access service provider” as having the meaning given that term in s 231(e)(4) of the Communications Act of 1934 (47 USC 231(e)(4)). That section defines “Internet access service” as “a service that enables users to access content, information, e-mail, or other services offered over the Internet, and may also include access to proprietary content, information, and other services as part of a package of services offered to consumers”.

[231] See, in particular, s 5(a)(1), 5(b) or 5(d) or pattern or practice that violates paras (2), (3), (4), or (5) of s 5(a), (b), and (d) of the CAN-SPAM Act.

[232] Id s 7(g)(1). These include: to enjoin further violation by the defendant (see s 7(g)(1)(A) of the CAN-SPAM Act); also to recover damages in an amount equal to the greater of: (i) actual monetary loss incurred by the provider of the Internet access service as a result of such violation; and the amount determined under para (3).

[233] In general for purposes of para (1)(B)(ii) of s 7(g)(3) of CAN-SPAM Act the amount determined under this paragraph is the amount calculated by multiplying the number of violations committed. The section deals with the action by the IASP, and it provides for the following: an amount of up to $100 for a violation of s 5(a)(1), or up to $25 for any other violation of s 5 (see s 7(g)(3)(A)(i and ii)).

[234] Id s 7(g)(3)(c).

the violation wilfully and knowingly,[235] and/or the defendant's unlawful activity included one or more of the aggravated violations set out in section 5(b).[236] In assessing damages, the court may consider whether:[237] the defendant has established and implemented with due care commercially reasonable practices and procedures designed effectively to prevent such violations;[238] or the violation occurred despite commercially reasonable efforts to maintain compliance with the practices and procedures to which reference is made in clause (i).[239] In an action brought under paragraph (1), the court may, in its discretion, require an undertaking for the payment of the costs of such action and assess reasonable costs, including reasonable attorneys' fees, against any party.[240]

6.3.2.5 Other provisions related to regulating unsolicited e-mail messages

(a) Do-not-e-mail registry

Section 9 of the CAN-SPAM Act provides for a do-not-e-mail registry.[241] Six months after the coming into operation of the CAN-SPAM Act, the Commission sent a report to various agents setting out a plan and timetable for establishing a nationwide marketing do-not-e-mail registry.[242] The report included an explanation of any practical, technical, security, privacy, enforceability, or other concerns that the Commission had regarding such a registry.[243] It further outlined how the registry would operate as regards children with e-mail addresses.[244] Authorisation to implement was granted nine months after the date of the enactment.[245]

[235] Id s 7(g)(3)(c)(i).

[236] Id s 7(g) and s 7(g)(3)(c)(ii). There is also a limitation on the penalty for any violation of s 5 (other than a violation of s 5(a)(1)) in that the amount determined under subparagraph (A) may not exceed $1 000 000. See s 7(g)(3)(B).

[237] Id s 7(g)(3)(D).

[238] Id s 7(g)(3)(D)(i).

[239] Id s 7(g)(3)(D)(ii).

[240] Id s 7(g)(4).

[241] See s 9(a) of the CAN-SPAM Act.

[242] Id s 9(a)(1).

[243] Id s 9(a)(2).

[244] Id s 9(a)(1-3).

[245] Id s 9(b).

In 2004, having sought and received input from various sources, the FTC rejected the list on the basis that it would lack an authentication system for e-mail.[246] Based on the input from those consulted, the Commission determined that "spammers would most likely use the registry as a mechanism for verifying the validity of e-mail addresses, and without authentication, the Commission would be largely powerless to identify those responsible for misusing the registry".[247] This aside, the registry-type solution to spam would raise serious security, privacy, and enforcement difficulties.[248]

Balough[249] is of the view that the do-not-spam registry will exacerbate the problem of spam in the sense that once an e-mail address is in that registry, it is virtually guaranteed that the person is alive and using that inbox.[250]

(b) Improving enforcement by providing rewards for information about violations

Section 11 of the CAN-SPAM Act required that within nine months after the date of the enactment, a report on a system of rewarding those who supply information about violations of the Act be issued.[251] This included procedures for the Commission to grant rewards of not less than twenty per cent of the total civil penalties collected for a violation of the Act to the first person who identified the person in violation of the Act[252] and those who supplied information which led to the successful collection of a civil penalty by the Commission.[253] The report also had to

[246] See Federal Trade Commission 'National do not e-mail registry: a report to congress (2004) the executive summary' 1-60 https://www.ftc.gov/sites/default/files/documents/reports/can-spam-act-2003-national-do-not-email-registry-federal-trade-commission-report-congress/report.pdf (date of use: 30 December 2015).

[247] Ibid.

[248] Ibid.

[249] See Balough (2003) 22/1 *Journal of Computer and Information Law* 87.

[250] Ibid 95; and Bolin supra n 67 426-8 for a discussion of the problems surrounding do-not-spam lists.

[251] See s 11(1) of the CAN-SPAM Act.

[252] Id s 11(1)(A).

[253] Id s 1. Also Platt Majoras D et al 'A CAN-SPAM Informant Reward System: A Report to Congress' (September 2004) for an executive summary of the report 1-74 https://ftc.gov/sites/default/files/documents/reports/can-spam-informant-reward-system-federal-trade-commission-report-congressexpert-reports/040916rewardsysrpt.pdf (date of use: 30 December 2015).

[253] 1(1)(A)(i).

establish procedures to simplify the process for submitting complaints on violations of the Act, including procedures to allow for the electronic submission of complaints to the Commission.[254] The report was compiled to consider key issues that should be included in establishing a reward system.[255] Recommendations were made on the features or elements that a potentially effective reward system would need to incorporate should Congress decide to implement one.[256] The following elements were identified: eligibility should be linked to the imposition of a final court order, rather than to the collection of civil penalties;[257] reward payments should be funded through appropriations rather than based on collected civil penalties; eligibility for rewards should be targeted at persons with high-value information; and reward determination should be wholly within the FTC's discretion and not subject to administrative or judicial review.[258]

(c) The effects of the CAN-SPAM Act

Not later than 24 months after the date of enactment of the CAN-SPAM Act, the Commissioner, in consultation with the Department of Justice and other appropriate agencies, was required to submit a report to Congress giving a detailed analysis of the effectiveness and enforcement of the provisions of the Act including the need (if any) for Congress to modify those provisions.[259] An analysis of recommendations was also to be included.[260] The above provision has illustrated how the CAN-SPAM

[254] Id s 11(1)(A)(ii).

[255] See Platt Majoras D et al 'A CAN-SPAM Informant Reward System: A Report to Congress' supra n 253.

[256] Id 19-32. The following key issues were considered in setting forth a reward system: "how could a reward system improve enforcement of the CAN-SPAM Act? Who are the potential informants who could identify the CAN-SPAM Act violators and supply valuable information leading to successful law enforcement action? What are the incentives and counter-incentives that would likely influence potential informants et cetera?".

[257] Id 33-42. The following are to be strongly considered: "it should be specified that it is unlawful to provide false information in connection with the reward system; protection of informants' identities should be provided allowing them to remain anonymous whenever testimony is not necessary for case prosecution; and it should be explicitly stated that the FTC cannot grant immunity".

[258] Ibid.

[259] See s 10(a) of the CAN-SPAM Act.

[260] Id s 10(a)(1). These recommendations included: "the extent to which technological and marketplace developments, including changes in the nature of the devices through which consumers access their e-mail messages, may affect the practicality negotiations and effectiveness of the provisions of the Act; how to address commercial e-mail that originates or is transmitted through or to facilities or computers in other nations, including initiatives or policy positions that the Federal Government could pursue through international negotiations, for

Act has been interpreted by the courts and how it is intended to protect consumers. It has also been noted that the CAN-SPAM Act draws most of its provisions from the state laws that preceded it. This is manifested by, among other elements, the CAN-SPAM Act's adoption of the opt-out mechanism which most states had followed in their legislation.

In what follows a commentary on the benefits derived from the CAN-SPAM Act; the criticisms levelled at the Act; and suggestions for improvement as raised by commentators are reviewed.

6.4 Commentary on the CAN-SPAM Act of 2003

6.4.1 Introduction

The discussion here focuses on how the CAN-SPAM Act has been perceived by a variety of commentators. There have been different reactions to the Act pointing to both positives and negatives, both its weaknesses and strengths. All perspectives are considered in assessing whether or not the CAN-SPAM Act is effective in protecting consumers.

6.4.2 Benefits of the CAN-SPAM Act

Various benefits are set to flow from the CAN-SPAM Act which include, but are not limited to, the fact that any law which regulates spam is better than no law at all.[261] The Act leaves room for future change, and this it is a good step in the fight against spam.[262] Proponents of the Act find that its alleged weaknesses are in fact its strength.[263] The CAN-SPAM Act serves to deter spammers from sending fraudulent or misleading e-mail messages, from concealing their identities, and from using

organizations, or institutions; and options for protecting consumers, including children, from the receipt and viewing of commercial e-mail that is obscene or pornographic". Also s 10(a) (2) and 10(a)(3) of the CAN-SPAM Act.

[261] See Yang (2004-2005) 4/1 *Chicago-Kent Journal of Intellectual Property* 12 ff*.*

[262] See Kikuchi supra n 151 311; and Brockhoeft (2004) 4/1 *Loyola Law and Technology Annual* 1.

[263] See Trussell (2004) 16/2 *Loyola Consumer Law Review* 183-5, where the author discusses the reactions to the CAN-SPAM Act.

intrusive methods to collect e-mail addresses.[264] Some note that the CAN-SPAM Act has made spam more “respectable” in that there are now set guidelines governing the transmission of direct e-mail solicitation.[265] Further, by overriding state laws, the CAN-SPAM Act is set to allow for easier enforcement as there are no conflicting jurisdictions which might create inconsistencies in defining spam.[266] While the above are positive comments, others see only problems and criticise various aspects of the Act.

6.4.3 Criticisms levelled against CAN-SPAM Act

Less positive commentators perceive the CAN-SPAM Act as weak and full of loopholes.[267] For them the Act is also vague, while for others it is harsh, or even under-enforced.[268] The following are among the criticisms levelled against the CAN-SPAM Act.

6.4.3.1 Pre-emption of state laws

(a) Background

Section 8 of the CAN-SPAM Act provides that the Act will supersede any state regulation or rule of a state, or political subdivision of a state, that expressly regulate the use of e-mail to send commercial messages.[269] Provision is made for an exception where state legislation, regulation, or rules prohibit falsification or deception in any part of a commercial e-mail message or information attached to the message.[270] Among the criticism advanced is that the provisions applicable in certain states allow for more stringent requirements and impose heavier penalties than

[264] Marks supra n 129 952 where the author discusses the strengths and weaknesses of the CAN-SPAM Act.

[265] This is a sentiment shared by marketers. See Ledbetter supra n 48 113.

[266] Ibid.

[267] Marks supra n 129 952.

[268] Ibid.

[269] See s 8(b)(1) of the CAN-SPAM Act of 2003.

[270] Id s 8(b). The federal law will not pre-empt the applicability of state laws that are not specific to e-mail, including state trespass, contract, or tort law; or other state laws to the extent that those laws relate to Acts of fraud or computer crime.

those under the CAN-SPAM Act, and that these too have been superseded.[271] Mobarek[272] noted that replacing the more stringent requirements with a mere prohibition on fraud, gives marketers a virtual green light to send spam to anyone they choose.[273] In addition, preventing the application of state laws significantly retards progress towards a resolution of the problem.[274] Furthermore, the supremacy of the CAN-SPAM Act applies only to those states that regulate commercial e-mail,[275] and the pre-emption clause contains broad exceptions for laws regulating falsification or deception which are not e-mail specific.[276] As is to be expected, preventing states from applying their state law has featured prominently in the courts.

(b) Selected case law on pre-emption

White Buffalo Ventures v University of Texas at Austin

The facts in the *White Buffalo Ventures v University of Texas at Austin* case[277] were briefly that the plaintiff, White Buffalo, offered online dating services for students at the University of Texas (UT) in Austin.[278] It sought an injunction against UT preventing the university from targeting and blocking its service e-mails as spam under the UT's information technology policy.[279] The district court denied the request for an injunction, and White Buffalo appealed claiming that the CAN-SPAM Act pre-empted the UT's anti-spam policy. The appeal was upheld on the basis that the CAN-SPAM Act had replaced state law.[280] The court held that the ambiguity in the

[271] See Alongi supra n 129 287; Cain (2007-2008) 3 *Journal of Law and Policy for the Information Society* 751 ff; and Brockhoeft supra n 262 40-2. For example, California state law had a stricter regulation prohibiting spam with its opt-in laws and also gave individuals a private right to bring suit for damages of up to $ 1 million (see California Business & Professional Code s 17529.2).

[272] Mobarek (2004) 16/3 *Loyola Consumer Law Review* 263.

[273] Ibid.

[274] Ibid.

[275] See Helman (2009) 50 *Boston College Law Review* 1539; and Mutchler (2010) 43 *Suffolk University Law Review* 966-8.

[276] Sorkin (2003) supra n 4 11.

[277] *White Buffalo Ventures v University of Texas at Austin* 420 F 3d 366 (5th Cir 2005) 1-13 http://www.openjurist.org/420/f3d/366/white-buffalo-ventures-llc-v-university-of-texs-at-austin (date of use: 30 December 2015). Hereafter '*White Buffalo* case'.

[278] Id 1-2.

[279] Id 3.

[280] Id 4-8.

CAN-SPAM Act exempted state-run ISPs from its purview and allowed them to implement the filtering systems.[281] Helman[282] notes that "by expressly pre-empting state regulation while at the same time expressly exempting ISPs from pre-emption, the court failed to take into account situations where those two entities are one and the same as noted in the facts".[283] Szabo[284] points out that the court here "failed to interpret the law correctly and so created a situation where states could face competing e-mail restrictions which could ultimately endanger the functionality of the Internet".[285]

Beyond Systems Inc v Keynetics Inc

In *Beyond Systems Inc v Keynetics Inc*[286] the plaintiff, Beyond Systems, alleged that it had received over 6 000 e-mail messages from the defendants, all of which were false and misleading with regard to their origin, transmission path, or subject line information.[287] The plaintiff also alleged that the defendant spammers conspired to send the unsolicited bulk e-mail in violation of the Maryland Commercial E-mail Act (MCEMA).[288] A broad reading of the exemption provision was followed when the US District Court of Maryland held that the MCEMA was not inconsistent with the CAN-SPAM Act.[289] The court held that because the MCEMA regulated falsified and deceptive header information in the e-mail message it did not frustrate the goals of the federal legislation and fell within the exemption provision in the CAN-SPAM Act.[290]

Omega World Travel Inc v Mummagraphics

[281] Id 8-13.

[282] See Helman supra n 275 1543-4 where the case is discussed.

[283] Ibid.

[284] See Szabo (2006) 7 *Texas Review of Entertainment & Sports Law* 72-5 for a discussion of this case.

[285] Ibid.

[286] See *Beyond Systems Inc v Keynetics Inc* 422 F Supp 2nd (2006) 1-60 http://www.steptoe.com/assets/attachments/1923.pdf (date of use: 30 December 2015). Hereafter '*Beyond Systems* case'.

[287] Id 1-12.

[288] See s 14.3001 of the MCEMA.

[289] *Beyond Systems* case supra n 286 27-29; and Helman supra n 275 1540-1.

[290] Ibid *Beyond Systems* case.

The applicant in *Omega World Travel Inc v Mummagraphics*[291] brought a case seeking damages from the defendants affiliated to Omega World Travel for spam e-mails advertising vacation packages allegedly sent by the defendants.[292] The claim was brought under the CAN-SPAM Act and the Oklahoma statute which provided that:[293]

> it shall be unlawful for a person to initiate an e-mail message that the sender knows, or has reason to know misrepresents any information in identifying the point of origin or transmission of the e-mail message. And does not contain information identifying the point of origin or the transmission path of the e-mail message, or contains false, malicious, or misleading information which purposefully or negligently injures a person.

The court had to decide whether the Oklahoma statute fell within the CAN-SPAM Act's exception for state laws governing commercial e-mail. The Fourth Circuit court upheld the lower court's ruling that, to the extent that the Oklahoma statute penalised non-material errors, it did not fall within the exception and could therefore not be applied.[294] Certain commentators have suggested that this case shows that statutes will not survive the CAN-SPAM Act pre-emption analysis if they can be interpreted as going beyond the material "falsification or deception" prohibition in commercial e-mail message or attachments.[295]

Gordon v Virtumundo

The facts in *Gordon v Virtumundo*[296] were briefly that Gordon managed Omni Innovations, a business that provided software development services which discouraged the act of spamming.[297] In connection with this business, Gordon established e-mail accounts and registered and maintained an Internet domain name "gordonworks.com" through "GoDaddy.com", a domain name he used to attract the attention of spammers.[298] Gordon began suing companies that were sending him spam under the CAN-SPAM Act and under Washington State's commercial e-mail

[291] See *Omega World Travel v Mummagraphics* 469 F 3d 348 94th Cir (2006) http://openjurist.org/469/f3d/348/omega-world-travel-incorporated-v-mummagraphics-incorporated-w (date of use: 30 December 2015). Hereafter '*Omega World Travel* case'.

[292] Id paras 1-9.

[293] See s 776.1A of the Oklahoma Statutes.

[294] *Omega World Travel* supra n 291 paras 29-46.

[295] See Wong (2007) 20/2 *Harvard Journal of Law & Technology* 459 ff.

[296] See *Gordon v Virtumundo* 575 F 3d 1040 (2009 US App LEXIS 17518) 1-28 http://www.nyls.edu/wp-content/uploads/sites/141/2013/08/575-F.3d-1040-Gordon-v.-Virtumundo.pdf (date of use: 30 December 2015). Hereafter '*Gordon's* case'.

[297] Id 3-4.

[298] Ibid.

statutes.[299] The question before the court was to what extent Gordon's claims based on the Washington State statutes had been pre-empted by the CAN-SPAM Act.[300] The United States Court of Appeals for the Ninth Circuit addressed the question of standing comprehensively, and held that the claims based on the Washington State statutes had been pre-empted by the CAN-SPAM Act. The judge interpreted these provisions as going beyond the CAN-SPAM Act's prohibition on falsification and deception.[301]

6.4.3.2 Regulation, not prohibition

The CAN-SPAM Act is sometimes referred to as the "you-can-spam Act", even though the Act is regarded as a pro-consumer measure which allows consumers to choose to stop receiving further unsolicited spam e-mail, it also allows spam and does not classify all spam as illegal.[302] The CAN-SPAM Act is also said to have legalised unsolicited commercial e-mails provided that they meet the requirements it sets.[303] While the CAN-SPAM Act has been said to protect consumers, it is also said to have failed to provide the most fundamental element of any anti-spam law – the prohibition of spam.[304] It is seen to have failed in that while it was intended to reduce the volume of unsolicited e-mail, the statute has instead facilitated a dramatic increase in both the amount of spam and the percentage of overall e-mail qualifying as spam.[305]

The CAN-SPAM Act fails to offer an effective solution to the enormous spam problem in that it allows the sender to invade in-boxes, and also forces spam recipients to take positive action to curtail future invasions.[306] Even though anti-spam

[299] See s 19.190.030 of the Washington Revised Code. This section deals with unsolicited or misleading electronic mail and violation of Consumer Protection Act (USA).

[300] *Gordon's* case supra n 296 5-6.

[301] Ibid 5-15 and Susuk (2010) 6/2 *Washington Journal of Law Technology and Arts* 161-9 ff for the effects this case will have on the future of spam litigation.

[302] Rutenberg (2011-2012) 14/1 *Vanderbilt Journal of Entertainment and Technology Law* 230-4.

[303] Brockhoeft supra n 262 39-40.

[304] See Mossoff (2004) 19/2 *Berkley Technology Law Journal* 637.

[305] See Soma, Singer & Hurd (2008) 45 *Harvard Journal on Legislation* 197; and Sorkin (2003) supra n 4 11.

[306] See Marks supra n 129 953; also Mayer (2004) 31/1 *Journal of Legislation* 189; ibid Sorkin; and Brockhoeft supra n 262 42-3.

measures have been adopted, legislation on its own is insufficient to resolve the considerable problems resulting from spam.[307]

6.4.3.3 Limitation of right to claim

(a) Background

The CAN-SPAM Act has also been criticised for not allowing the individual the right to claim against the spammer – he or she must rely on the FTC to enforce his or her claim.[308] This right to sue is also limited to IASP who are "adversely affected" by the unsolicited communications.[309] In addition, the IASP must also prove that the defendant exhibited a pattern or practice in its delivery of unsolicited e-mail.[310] The IASP must prove the defendant's liability and the relief provided can result in an injunction or damages amounting to the greater of actual or statutory damages, which are often not collected in full.[311]

Certain commentators argue for the traditional self-help role of individual litigation to be resurrected to tackle the modern communication problems as that will have a real impact on stemming the tide of unwanted commercial e-mail by both businesses and individuals.[312] These private rights, it is argued, could create a "self-sustaining" anti-spam system through which individuals could seek recourse without having to rely on ISPs, state attorneys, and government agencies for enforcement.[313] This right of action will only be effective against spammers who are caught and found liable.[314]

[307] See Trussell supra n 263 187.

[308] See Bolin supra n 67 415; Cain supra n 271 760; Ledbetter supra n 48 115-6; and Reid (2010) 4 *Akron Intellectual Property Journal* 305.

[309] Lorentz supra n 152 574 and 584-6; also Susuk supra n 301 159-61 and 168-9 where the author lists the following as the decisions neutralising the private rights: "(a) the threshold question of whether a plaintiff is an IASP involves close judicial scrutiny regarding its underlying purpose; (b) if the plaintiff is an IASP it must show that it suffered significant IAS type harm above and beyond ordinary inconveniences from a normal spam volume; (c) should the plaintiff's CAN-SPAM claim fail, the viability of a parallel state claim is now highly questionable; and (d) if the court determines that the claim is frivolous, the plaintiff runs the risk of being responsible of the defendant's legal fees and costs".

[310] Ibid.

[311] Lorentz supra n 152 584-6; and Helman supra n 275 1543.

[312] See Cain supra n 270 776; Id Lorentz 603-4; and Soma, Singer & Hurd supra n 305 197.

[313] Id Soma, Singer & Hurd 193-5 where the authors discuss the issue of allowing individuals to sue spammers for statutory damages.

[314] Ibid.

(b) Selected case law

Gordon v Virtumundo

In *Gordon v Virtumundo*[315] the court held that the plaintiff met two requirements: that it must be an IAS; and that it must actually have been "adversely affected" which is one of the violations in the CAN-SPAM Act.[316]

Spam Arrest LLC v Replacements Ltd

The facts in *Spam Arrest LLC v Replacements Ltd*[317] were briefly that Spam Arrest offered a subscription to an anti-spam service that blocked e-mails from senders until they had been verified.[318] To verify senders, Spam Arrest e-mails a link to a verification page where the sender can click the verify button. The verification page contains a two paragraph "sender agreement"[319] which specifies that clicking the verify button indicates consent to the sender agreement.[320]

The court found that Spam Arrest could not show that the defendant, Sentient Jet, had sent unsolicited commercial e-mail. It also held that Spam Arrest bore the burden of showing that Sentient Jet had not received the consent of the e-mail recipients to send them e-mail, despite Sentient being required to prove that recipients had consented to its e-mail.[321]

[315] *Gordon's* case supra n 296 10-15.

[316] Ibid. See the facts of this case in pars 6.4.3.1 (b) above.

[317] *Spam Arrest LLC v Replacements Ltd* (2013) WL 4675919 (WD Wash Aug 29 2013) 1-36 https://cases.justia.com/federal/district-courts/washington/wawdce/2:2012cv00481/182956/96/0.pdf?ts=1377958938 (date of use: 30 December 2015), hereafter '*Spam Arrest* case'; and Goldman E 'Anti-spam lawsuits rarely win, as highlighted by a recent loss by spam arrest' http://www.forbes.com/sites/ericgoldman/2013/09/12/anti-spam-lawsuits-rarely-win-as-highlighted-by-a-recent-loss-by-spam-arrest/ (date of use: 30 December 2015) where the author comments on the *Spam Arrest* case.

[318] Ibid *Spam Arrest* case.

[319] The sender agreement made senders promise that they were not sending unsolicited commercial e-mail and specified that senders had to pay $2000 for each violation of the agreement.

[320] *Spam Arrest* case supra n 317 1-36; and *Beyond Systems INC v Kraft Foods Incorporated* No 13-2137 (July 21 2014) 1-13 http://caselaw.findlaw.com/us-4th-circuit/1691263.html (date of use: 30 December 2015).

[321] Ibid *Spam Arrest* case.

Wagner v Spire Vision

In *Wagner v Spire Vision*[322] the plaintiff alleged that he had received 49 spam e-mails all containing materially falsified, misrepresented, and forged information in violation of California's anti-spam law.[323] The defendants had allegedly registered their domain names and those used to send spam to unregistered fictitious business names.[324] The court noted that in order for Wagner to prevail he had to show that the header information in the e-mails not only violated the California statute, but also contained material misrepresentations to avoid pre-emption under the CAN-SPAM Act.[325] It was held that the plaintiff had not proven the merit of his claims under section 17529.5 of the California Business and Professions Code.[326]

6.4.3.4 Global nature of spam

It is said that the CAN-SPAM Act will make enforcement more difficult considering that spam also originates from outside the US borders.[327] The main problem with enforcing the Act has been noted as an inability physically to locate spammers.[328] Daniel notes that the CAN-SPAM Act has not contributed to the resolution of problems relating to the global nature of spam, but that what it has achieved is that spammers have moved their operations offshore or use relays to make it appear as if they have moved.[329] Daniel further notes that this raises new problems such as: jurisdiction; enforcement of laws against offshore spammers; and the identification and location of international spammers,[330] and that tough spam regulation will compel spammers to move abroad.[331] Regarding enforcement, it is noted that since spammers are moving beyond the US borders in order to avoid compliance with the

[322] *Wagner v Spire Vision* C13-04952 WHA (ND Cal March 2014) 1-16 http://blog.ericgoldman.org/archives/2014/06/can-spam-preemption-doesnt-apply-to-fraud-and-more.htm (date of use: 30 December 2015). Hereafter '*Wagner's* case'.

[323] See s 17529.5 of the California Business and Professions Code n 6 above.

[324] *Wagner's* supra n 322 1-2.

[325] Id 5.

[326] Id 10-12.

[327] Ledbetter supra n 48 115-6; see also Chapter 4 4.4.2.3 (h) above on the global cooperation outreach.

[328] See Daniel (2005-2006) 94 *Kentucky Law Journal* 373.

[329] Ibid.

[330] Ibid. See also Dane (2006) 6 *Asper Review International Business & Trade Law* 251.

[331] Ibid Daniel. See also Helman supra n 275 1547-8.

CAN-SPAM Act, spam laws need to be adopted in other jurisdictions.[332] Ideally, there should be worldwide uniformity in anti-spam legislation,[333] with worldwide enforcement as recommended in the OECD's Spam Toolkit.[334] Incentives for those who cooperate in cross-border enforcement are also to be encouraged.[335] In attempting to remedy the situation solutions have been proposed to advance and improve the CAN-SPAM Act.

6.5 Solutions for improvements to the CAN-SPAM Act

6.5.1 Technology for enforcement

In addition to regulation through the CAN-SPAM Act, some commentators are of the opinion that the Act is ineffective without effective technology to identify e-mail senders, block unwanted e-mail, and determine an e-mail's country of origin.[336] The solution advanced is that in order to stop spam, private businesses engaged in developing technological solutions to block spam should hasten to develop the technology necessary to enforce the statute, which will include the ability to trace UCE to its source.[337]

The key to fighting spam is set to be vigorous enforcement in which the federal government strives to identify the spammers and prosecute them to the fullest extent of the law.[338] While technical approaches alone are not enough to solve the spam problem, market-based initiatives – including self-help mechanisms and spam filter systems – must be included, even if most of the time they merely delete spam.[339]

6.5.2 Inclusion of opt-in mechanism

It is also claimed that the solution to the eradication of spam lies in the introduction of restrictive mechanism such as opt-in mechanism in preference to the opt-out

[332] Lorentz supra n 152 601-603.
[333] Ibid.
[334] Id 599-600.
[335] Ibid.
[336] Ledbetter supra n 48 124-7 and Daniel supra n 328 375-7.
[337] Id Daniel 373-80.
[338] Brockhoeft supra n 262 43.
[339] Marks supra n 129 957-8.

mechanism.[340] Shames note that the effectiveness of the opt-out provisions in the CAN-SPAM Act may be questioned, it would appear to work more effectively in conjunction with the opt-in requirements where these are applied.[341] The opt-in mechanism will also serve to increase the efficiency of e-mail by allowing users easily to identify spammers, and so eliminate the need for the do-not-e-mail registry.[342] Balough notes that "the federal legislation should also adopt an opt-in mechanism with penalties that can be imposed not only against the spammer, but also in those web sites receiving the traffic generated by the unsolicited commercial e-mail".[343] In this regard, others argue that lessons can be learned from the international arena – especially as regards the opt-in mechanism – and that the USA should, therefore, look beyond its borders in order to strengthen its legislation regulating spam.[344]

6.5.3 A multi-faceted solution

Commentators in the USA have pointed to a multi-faceted approach to combat spam.[345] In order to create a tougher and more effective anti-spam statute, it has been stated that this multi-faceted solution should include redefining spam by broadening the definition to include all UCE,[346] and enacting minimum requirements for e-mail transmission on ISP networks.[347] ISPs should also be held accountable to other ISPs for actual damages, and individuals should be entitled to sue spammers for statutory damages.[348] Finally, international anti-spam efforts should be promoted.[349] It has also been mooted that the USA should assist in developing an effective spam- reduction scheme, and that in doing so it would be well advised to

[340] See Shames (2004) 66 *University of Pittsburgh Law Review* 396-403 and 408 where the author discusses the advantages, constitutionality, and effects of such a mechanism. Shames also note that: "this would require senders of unsolicited commercial e-mail to obtain the permission of recipients before sending them commercial solicitations".

[341] Ibid.

[342] Kikuchi supra n 151 313.

[343] See Balough supra n 249 95.

[344] Kikuchi supra n 151 295-311 where the author notes that: "the USA should follow Japan and the European Union as examples of change, or incorporate some of the provisions from those jurisdictions that work". See too Mutchler supra n 275 968-79 where the author compares the USA and EU and Lorentz supra n 152 603.

[345] See Soma, Singer & Hurd supra n 305 197; and Marks supra n 129 958.

[346] Ibid.

[347] Ibid.

[348] Ibid.

[349] Ibid.

look to Nigeria which has implemented both technological and legislative measures in its attempt to halt the proliferation of spam.[350] Another way to stop spam e-mails is to have a worldwide, integrated system which includes countries, ISPs, individuals, and law enforcement agencies, all cooperating to make spam a less attractive marketing tool.[351]

6.5.4 International cooperation

6.5.4.1 Background

As part of a multi-faceted solution to combat spam, countries have entered into partnership agreements with stakeholders in different countries. The USA has signed a number of Memorandum of Understanding[352] with other agencies and organisations in different countries aimed at collaborating in the fight against spam. This is also what the ITU and OECD advocates as noted in chapter 4 above.

6.5.4.2 Memorandum of Understanding between the USA and other countries

(a) United States, United Kingdom, and Australia

In 2004 the USA, the United Kingdom, and Australia joined forces by signing a MoU in which they undertook to share resources to fight spam.[353] This MoU noted that the convenience and efficiency of e-mail is threatened by the extremely rapid growth in the volume of unsolicited commercial e-mail which often contains deceptive content

[350] Nigeria which was considered a gateway for spam in 2002 began working with one of its companies to develop an anti-spam solution to stop outbound spam e-mails and also mandated its ISPs to install outbound e-mail filtering. See Alepin (2004-2005) 28 *Columbia Journal of Law & the Arts* 70.

[351] See Mutchler supra n 275 981.

[352] Hereafter 'MoU'.

[353] See *Memorandum of Understanding on Mutual Enforcement Assistance in Commercial E-mail Matters Among the Following Agencies of the United States, the United Kingdom, and Australia: The United States Federal Trade Commission; The United Kingdom's Office of Fair Trading, the United Kingdom's Information Commissioner, Her Majesty's Secretary of the State for Trade and Industry in the United Kingdom, the Australian Competition and Consumer Commission, and the Australian Communications Authority* (02 July 2004) 1-11 http://www.ftc.gov/sites/default/files/attachments/international-antitrust-and-consumer-protection-sooperation-agreements/050224memounderstanding.pdf (date of use: 30 December 2015)). Hereafter 'MoU USA, UK and Australia'.

or material that many recipients may consider offensive.[354] As a result, the parties recognised their need to share evidence which will facilitate the effective enforcement of spam violations.[355] Parties agreed on the following issues:[356] cooperation in detecting and investigating spam violations or suspected spam violations; research, consumer and business education; and law enforcement with regard to spam violators. The signatories further undertook to keep each other informed of developments having a bearing on the MoU in their respective countries.[357]

(b) USA and Mexico

The FTC and Mexico's Consumer Protection Agency, *Procuraduria Federal Del Consumidor* (PROFECO) signed a bilateral MoU in January 2005 to promote enhanced cooperation in the fight against cross-border fraud.[358] This document was the first consumer protection MoU signed by the FTC with a non-English-speaking nation.[359] The MoU strengthens the close relationship between the USA and Mexico and will facilitate greater law enforcement coordination in consumer protection matters affecting both nations.[360] The following key goals were established by this MoU: notification of enforcement activities; cooperation and coordination; and exchange of information.[361]

(c) USA and Spain

[354] Id 1.

[355] Id 4-6 for the objects and scope of assistance.

[356] Ibid.

[357] Id para II B.

[358] See *Memorandum of Understanding on Mutual Assistance in Consumer Protection Matters between the Federal Trade Commission of the United States of America and the Procuraduria Federal del Consumidor (Office of the Federal Attorney for Consumer Protection) of the United Mexican States* (2005) 1-7 http://www.ftc.gov/sites/default/files/attachement/international-antitrust-and-consumer-protection-cooperation-agreements/050127/memounderstanding.pdf (date of use: 30 December 2015). Hereafter 'MoU USA and Mexico'.

[359] See Federal Trade Commission 'FTC signs memorandum of understanding with the Mexican consumer Protection body' http://www.ftc.gov/news-events/press-releases/2005/01/ftc-signs-memorandum-understanding-mexican-consumer-protection (date of use: 30 December 2015).

[360] Ibid. This memorandum is considered a "best effort" agreement and does not legally bind nor alter either country's existing consumer protection laws.

[361] See scope of assistance of the MoU USA and Mexico supra n 358 3-4.

In February 2005 the USA signed another MoU, this time with Spain, aimed at promoting enhanced cooperation and information-sharing on spam enforcement activities.[362] Signatories recognised that it is in their common interest to share evidence that will facilitate effective enforcement for spam violations.[363] Also included is: the facilitation of research and business education on spam, and the promotion of a better understanding of the participants economic; legal conditions and theories as regards spam violations.[364]

(d) USA and Nigeria

On 28 August 2013 the FTC signed a MoU with two Nigerian agencies to increase cooperation and communication in their joint efforts to stamp out cross-border fraud.[365] This is the first FTC MoU to include a foreign criminal enforcement authority.[366] The signatories observed that cross-border scammers use fraudulent bulk e-mails and other scams to reach consumers the world over. This MoU is said to help the agencies to protect consumers in both the USA and Nigeria.[367] It will also address the scourge of cross-border scams using fraudulent e-mails, and other deceptive scams used to send bulk e-mails to consumers.[368]

The MoU noted the need to create "the needed synergy and cooperation to fight such fraudulent and deceptive practices which are detrimental to the interests of

[362] See *Memorandum of Understanding on Mutual Enforcement Assistance in Commercial e-mail Matters between the Federal Trade Commission of the United States of America and the Agencia Espanola De Proteccion De Datos.* Document (2005) 1-9 http://www.ftc.gov/sites/defaults/files/attachments/international-antitrust-and-consumer-protection-cooperation-agreements/050224memounderstanding.pdf (date of use: 30 December 2015). Hereafter 'MoU USA and Spain'.

[363] Ibid.

[364] Id 3. For the object and scope of assistance see MoU USA and Mexico supra n 358 3-5.

[365] See *Memorandum of Understanding between US FTC and the Federal Republic of Nigeria's Consumer Protection Council (CPC) and Economic and Financial Crimes Commission (EFCC) on Mutual Enforcement Assistance in Consumer Protection Matters* 1-10 (2013) http://www.ftc.gov/news-events/press-releases/2013/08/ftc-signs-memorandum-understandu =ing-nigerian-consumer-protection (date of use: 30 December 2015). Hereafter 'MoU USA Nigeria'.

[366] This Day Live 'CPC, EFCC, US Agency sign on consumer protection' http://www.thisdaylive.com/articles/cpc-efcc-us-agency-sign-mou-on-consumer-protection/157613 (date of use: 30 December 2015). The CPC addresses consumer complaints through investigations and enforcement and the EFCC is a criminal enforcement agency with authority to address consumer fraud and other financial crimes.

[367] Ibid; and MoU USA and Nigeria supra n 365 2-4 for the objectives and scope of assistance.

[368] Ibid.

genuine businesses and consumers".[369] It also covers the following issues: information-sharing in investigations and law enforcement proceedings; civil or criminal investigation assistance; intelligence gathering; and the use of complaint data.[370] Consumer education is also addressed and a joint implementation committee for performance under the MoU by the collaborating agencies is created.[371]

(e) USA and UK

On 6 March 2014 the FTC and the UK Privacy Enforcement Agency signed an MoU to promote increased cooperation and communication between the two agencies in an effort to protect consumer privacy.[372] The MoU is designed "to bolster these countries' privacy enforcement partnership at the time when consumer information is moving across national borders, increasing the need for cross-border enforcement cooperation".[373] The MoU's aim is to provide mutual assistance and exchange of information for purposes of investigating, enforcing, and/or securing compliance with privacy laws, which includes the sharing of complaints and the provision of investigative assistance.[374] The MoU also covers the enforcement of privacy laws in both countries,[375] and signals regulators' increasing efforts at cross-global enforcement, particularly as regards issues of privacy.[376]

[369] Ibid.

[370] Ibid.

[371] MoU USA and Nigeria supra n 365 2-4.

[372] See *Memorandum of Understanding between the United States Federal Trade Commission and the Information Commissioners Office of the United Kingdom on Mutual Assistance in the Enforcement of Laws Protecting Personal Information in Private Sector.* Document accessed (2014) 1-10 http://www.ftc.gov/systems/files/attachments/international-competition-consumer-protection-cooperstion-agreements/140306ftc-uk-mou.pdf (date of use: 30 December 2015). Hereafter 'MoU USA and UK'.

[373] Ibid.

[374] Id 4-6 for the objects and scope of the MoU.

[375] These privacy laws include: Federal Trade Commission Act of 1914 as amended; Fair Trade Reporting Act of 1970; CAN-SPAM Act of 2003 among others (Federal Trade Commission USA); and Data Protection Act of 1998 and Privacy and Electronic Communications (EC Directive) Regulations (Information Commission Office in UK). See Olshanlaw 'FTC and UK Head sign MOU signaling cross border Privacy enforcement' http://www.olshanlaw.com/blogs-Advertising-Law-blog,FTC-UK-Cross-Border-Privacy (date of use: 30 December 2015).

[376] See MoU USA and UK supra 372 1-10.

The MoUs above are subject to review regarding the cooperation, coordination, and enforcement assistance undertaken by the parties.[377] However, it will be best for parties involved to do their part in combating spam by adopting some of the provisions in the MoUs.

6.6 Concluding remarks

In this chapter a discussion of the USA's anti-spam laws was outlined. In the discussion it is noted how the anti-spam law came to being – from regulation at state level to the federal CAN-SPAM Act. It was pointed out that although the federal law pre-empts state laws, it also drew a number of its provisions from state legislation. Criticism of the federal Act was also highlighted.

This chapter has also shown how the CAN-SPAM Act provisions have been interpreted by the courts, and suggestions on addressing the problems by other commentators were identified. Nationally, the USA's CAN-SPAM Act reflects basic elements that are necessary in any anti-spam legislation. Even though the USA has chosen the opt-out mechanism, it has also outlined the process and the time frames for the implementation of such a mechanism.

It further emerged that spam is both a national and an international problem. In addressing the call to combat spam at a global level, the USA appears to have followed the route of entering into individual MoUs with agencies or organisations in various countries. While these agreements are not binding, they are a step in the right direction and indicate recognition among countries that spam is indeed a global problem which can be overcome only by a multi-faceted solution.

In the following chapter an examination on the Australian approach to the issue of spam will be addressed.

[377] See MoU USA and Spain supra n 362 8; also MoU USA, UK and Australia supra n 353 10; and MoU USA and Mexico supra n 358 7.

CHAPTER 7

A COMPARATIVE STUDY OF ANTI-SPAM LAWS: AUSTRALIA

7.1 Introduction

Chapter 6 launched a discussion of anti-spam laws in the USA. In this chapter, focus will be on the second anti-spam jurisdiction by considering how the issue is regulated in Australia. Like the USA, Australia has been regulating spam since 2003. The Australian government has adopted a five-pronged strategy in its fight against spam namely: a multi-faceted initiative. This strategy includes strong legislation and enforcement within Australia; consumer and industry education; industry partnership; technology; and international cooperation.[1]

The discussion follows the strategy outlined above. When discussing the issue of "strong legislation" the following outline will be highlighted: the purpose of the legislation and the anti-spam provisions; a commentary on the Act taking into consideration the benefits of the Act; challenges posed on the legislation which includes criticism by commentators; and enforcement. Case law is integrated into the discussion of these issues. The four remaining initiatives will follow before offering some concluding remarks.

7.2 Anti-spam legislation in Australia

7.2.1 Background to Australia's anti-spam legislation

Before anti-spam legislation came into operation, Australia dealt with the issue in other related legislation.[2] Australia adopted its anti-spam law – the Spam Act[3] – on

[1] See ACMA 'Submission to Spam Act Review: ACMA*'* 5 http://www.acma.gov.au/webwr/consumer_info/spam/acma%20submission%20to%20review.pdf (date of use: 15 January 2016) and ACMA 'Fighting spam in Australia' http://www.acma.gov.au/theACMA/About/The-ACMA-story/Meeting-our-standard/fighting-spam-in-australia (date of use: 15 January 2016).

[2] For a background on the pre-anti-spam law in Australia see: Vaile (2004) 6/9 *Internet Law Bulletin* 113; Malcolm (2001) 12/2 *Journal of Law and Information Science* 242-9; Relf (2005) 2 *Macquarie J Bus L* 93-4; and Quo (2004) 11/1 *Murdoch University Electronic Journal of Law* 4-10 http://www.austlii.edu.au/au/journals/MurUEJL/2004/11.html (date of use: 15 January 2016).

[3] See Spam Act 129 of 2003.

12 December 2003 and assented to in April 2004.[4] The Spam Act addresses the three main requirements: first, consent before unsolicited communications can be sent, which, in turn, invokes the opt-in requirement making spam illegal and punishable by law in Australia; second, accurate sender information when unsolicited mail is sent to end users; and third, an unsubscribe facility in such e-mails.[5]

7.2.2 Purpose of the Spam Act

The aim of the Spam Act is: to reduce Australia's role as a source of spam, to minimise spam for Australian end users, and to extend Australia's involvement in worldwide anti-spam activities.[6] As noted by Australian Communications and Media Authority[7] the mission of the Spam Act is therefore to promote citizen confidence in electronic messaging as a means of commercial communication.[8] Note should be taken here that the Australian Communications Authority[9] and the ACMA are used interchangeably when discussing the issues below.

7.2.3 Anti-spam provisions under the Spam Act of 2003

7.2.3.1 Definitions

Section 4 of the Spam Act provides a list of definitions. While most of these definitions are highlighted when the relevant issues are considered below, the following definitions are outlined here for ease of reference.

[4] The Act came into operation 120 days after it was signed into law in April 2004. See Vaile supra n 2 113. The Act was also rolled out in phases starting from 12 December 2003 and ending on 10 April 2004 (see s 2 of the Spam Act of 2003).

[5] See Australian Government Department of Communications Information Technology and the Arts 'Spam Act 2003: A practical guide for government' http://www.acma.gov.au/webwr/consumer_info/spam/spam_act_pracguide_govt.pdf (date of use: 15 January 2015).

[6] See ACMA 'Meeting the ACMA standard: fighting spam in Australia' http://acma.gov.au/theACMA/About/The-ACMA-story/Meeting-our-standard/fighting-spam-in-australia (date of use: 15 January 2016).

[7] Hereafter 'ACMA'. The ACMA is the independent statutory authority tasked with ensuring most elements of Australian's media and communications legislation related regulation and numerous derived standards and codes of practice operate effectively and efficiently and in the public interest. See ACMA 'Introduction to the ACMA' http://www.acma.gov.au/theACMA/About/The-ACMA-story/Communicating/introduction-to-the-acma (date of use: 15 January 2016).

[8] Ibid.

[9] Hereafter 'ACA'. ACA and ACMA will be used interchangeably.

(a) Commercial electronic message

A "commercial electronic message"[10] is defined as "an electronic message where, having regard to its content, the way in which it is presented, and the content that can be located using the links, telephone numbers, or contact information (if any), are set out".[11] The purpose(s) of the message is listed in section 6(1) of the Spam Act which includes, among others, the advertising, promotion and supply of goods and services.[12]

Like the USA above, the term "spam" in Australia is classified in relation to the content of the message as "commercial" and not its volume or "bulk" (or number of messages actually sent). The definition of CEM covers e-mails, mobile phone messaging (SMS, MMS, and EMS), and instant messaging of a commercial nature.[13] The Spam Act does not apply to facsimile messages, Internet pop-ups, or voice-to-voice telemarketing.[14]

(b) Electronic messages

An "electronic message" is "a message sent using an Internet carriage service or any other listed carriage service".[15] It is also an electronic address related to an e-mail account, an instant messaging account, a telephone account, or any similar account.[16] In terms of the Spam Act it is immaterial whether the electronic address exists,[17] or whether the message reaches its intended destination.[18] However, if a message is sent by way of voice call made using a standard telephone service, the

[10] Hereafter referred to 'CEM'.

[11] See s (6)(1)(a-c) of the Spam Act of 2003.

[12] Ibid s 6(1)(d-p) where other purposes are listed as: "offering, advertising or promoting the supply of land or interest of land; and also assisting or enabling, by deception, to dishonestly obtain property belonging to another person; obtaining a financial advantage from another person; or obtaining gain from another person".

[13] ACMA 'Australian eMarketing code of practice' http://acma.gov.au/Industry/Marketers/Anti-Spam/Ensuring-you-dont-spam/australia-emarketing-code-of-practice-ensuring-you-dont-spam-i-acma (date of use: 15 January 2016).

[14] Ibid.

[15] See s 5(1)(a) of the Spam Act. The term "message" is defined in s 4 of the Spam Act as "information whether in the form of text; data; speech, music or other sound; visual images; any other form; or any combination of forms".

[16] Id s 5(1)(b).

[17] Id s 5(2).

[18] Id s 5(3).

message would not be considered an electronic message for purposes of the Spam Act.[19]

7.2.3.2 Rules for sending electronic mail

Section 3 of the Spam Act provides a simplified outline of the Act which establishes a scheme to regulate commercial e-mail and other types of CEM. This outline includes:[20]

> the prohibition of the dissemination of unsolicited commercial electronic messages;[21] provides for CEMs to include information about the individual or organisations who authorises the sending of the message; demands that commercial electronic messages contain a functional unsubscribe facility; prohibits the supply, acquisition, or use of address-harvesting software; prohibits the supply, acquisition, or use of an electronic address list produced using address-harvesting software; and provides civil penalties and injunctions as the principal remedies for breaches of the Act.

These requirements are found in Part 2 of the Spam Act which deals with the rules for sending CEMs.

(a) Prohibition on sending unsolicited commercial electronic messages

Section 16(1) of the Spam Act prohibits a person from sending or causing to be sent a UCEM that has an Australian link[22] and is not a designated CEM.[23] For the

[19] Id s 5(5).

[20] Id s 15 for the simplified outline of this part.

[21] Hereafter 'UCEM'.

[22] For purposes of the Spam Act a "CEM" has an Australian link if, and only if: "the message originates in Australia; or the individual or organisation who sent the message or authorised the sending of the message is: an individual who is physically present in Australia when the message is sent; or an organisation whose central management and control is in Australia when the message is sent; or the computer, server or device that is used to access the message is located in Australia; the relevant electronic account holder is: an individual who is physically present in Australia when the message is accessed; or an organisation that carries on business or activities in Australia when the message is accessed; or if the message cannot be delivered because the relevant electronic address does not exist, assuming that the electronic address existed, is reasonably likely that the message would have been accessed using a computer, server or device located in Australia".

[23] Schedule 1(2) of the Spam Act outlines the term "designated CEM" as: "the message that consists of no more than factual information (with or without directly related comment) and any or all of the following additional information: the name, logo, and contact details of the individual or organisation who authorised the sending of the message; The name and contact details of the author; if the author is an employee, the name, logo and contact details of the author's employer; if the author is a partner in a partnership the name, logo and contact details of the partnership; if the author is a direct or officer of an organization; if the message is sponsored, the name, logo and contact details of the sponsor; information required to be included by s 17 (that deals with CEMs which must include accurate sender information); information that would

purposes of the Spam Act, these designated CEMs can be authorised by different institutions including government bodies[24] and educational institutions.[25] The purpose of having a category of designated UCEMs is to ensure that there are no unintended restrictions on government-to-citizen or government-to-business communication, or any restriction on religious or political organisations.[26] The exclusion only applies if the relevant body is the supplier or prospective supplier of the goods or services concerned.[27]

Section 16(1) does not apply if: "the relevant electronic account holder consented[28] to the sending of the message;[29] or if the person[30] did not know, and could not with

have been required to be included by s 18 (that deals with CEMs which must contain a functional unsubscribe facility) if that section had applied to the message. Assuming that none of the additional information had been included in the message, the message would not have been a CEMs; and the message complies with such other condition or conditions (if any) as are specified in the regulations".

[24] Section 4 of the Spam Act defines the term "government body" as: "a department of the Commonwealth, a state or a territory; an agency, authority or instrumentality of the Commonwealth, a state or a territory; a department of government of a foreign country; an agency, authority or instrumentality of the government of a foreign country; a department of the government of a part of a foreign country; and an agency, authority or instrumentality of the government of a part of a foreign country". Other organisations included here are political parties, religious organisations, and charities (see cl 3 (a)-(c) of Schedule 1 to the Spam Act).

[25] See cl 4 (a)-(d) of Schedule 1 to the Spam Act. Section 4 of the Spam Act lists the following as educational institutions: a pre-school; a school; a college; and a university.

[26] See Relf supra n 2 101 and Bender MR 'Australia's spam legislation: a modern King Canute' (2006) 2-24 http://papers.ssrn.com/sol3/papers.cfm?abstract_id=916724 (date of use: 15 January 2016).

[27] Ibid.

[28] Schedule 2 (2) to the Spam Act defines the term "consent" as: "*express consent*: which takes place when an individual or organization first provides the e-mail address and if they plan to send the recipient CEMs then consent must be obtained. Express consent comprises the filling in a form; ticking a box on a web site; consent obtained either over a phone, face to face or by swapping business cards, as long as the recipient is aware they may receive commercial messages. One cannot send an electronic message seeking consent for this in itself is considered a commercial message because it seeks to establish a business relationship. *Inferred consent* can occur "via an existing business or other relationship, where there is reasonable expectation of receiving commercial electronic message; if the address is not accompanied by a statement saying "no commercial messages are wanted" the subject of the message is directly related to the role or function of the recipient. This happens through conspicuous publications if: the electronic address published is accessible to the public, or a section thereof (for example, it appears on a web site or in a telephone directory or brochure); the address is not accompanied by a statement that commercial messages are not wanted; and the subject matter of one's message is directly related to the principal role or function of the recipient (electronic account holder)". See ACMA 'Spam consent' http://www.acma.gov.au/Industry/marketers/Anti-Spam/Ensuring-you-dont-spam/spam-consent-ensuring-you-dont-spam-i-acma (date of use: 15 January 2016); also see Schedule 2(4) for instances when consent may be inferred from publication of an electronic address; and ACMA 'Inferred consent and conspicuous publications' http://www.acma.gov.au/theACMA/spam-inferred-consent-and-conspicuous-publications (date of use: 20 January 2015).

[29] See s 16(2) of the Spam Act.

[30] The term "person" is defined as including a partnership in s 4 of the Spam Act.

reasonable diligence have ascertained, that the message had an Australian link;[31] and if the person sent the message or caused the message to be sent by mistake".[32] A person must not send, or cause a CEM to be sent, to a non-existent electronic address if he or she does not have reason to believe that the electronic address exists.[33]

(b) Accurate sender information

Section 17 of the Spam Act prohibits a person to send, or cause to be sent, a CEM with an Australian link unless the message clearly and accurately identifies the individual or organisation that authorised its being sent.[34] The message must also include accurate information about how the recipient can readily contact that individual or organisation.[35] The information must also comply with the condition or conditions (if any), specified regulations, and that information should be reasonably likely to be valid for at least thirty days after the message is sent.[36]

(c) Functional unsubscribe facility

Section 18 of the Spam Act provides for a functional unsubscribe facility. This section provides that a person may not send, or cause to be sent, a CEM which:[37]

(a) has an Australian link;
(b) is not a designated commercial electronic message;
(c) unless the message includes: a statement to the effect that the recipient may use an electronic address set out in the message to send an unsubscribe message to the individual or organization who authorized the sending of the first mentioned message; or a statement to similar effect;[38]
(d) the statement is presented in a clear and conspicuous manner;

[31] See s 16(3) of the Spam Act.
[32] Id s 16(4).
[33] Id s 16(6)(a).
[34] Id s 17(1).
[35] Id s 17(1)(a).
[36] Id s 17(1)(1)(c) and (d); ACMA 'Sender identification' http://www.acma.gov.au/Industry/Marketers/Anti-Spam/Ensuring-you-dont-spam/sender-identification-ensuring-you-dont-spam-i-acma (date of use: 15 January 2016).
[37] Id s 18(1).
[38] Id s 18(1)(c) (i) and (ii).

(e) the electronic address is reasonably likely to be capable of receiving: (i) the recipient's unsubscribe message[39] (if any); and (ii) a reasonable number similar as unsubscribe messages sent by other recipients (if any) of the same message at all times during a period of at least 30 days after the message is sent;[40]

(f) the electronic address is legitimately obtained; and

(g) the electronic address complies with the condition or conditions (if any) specific in the regulations.

(d) Supply, acquisition, and use of harvesting software or lists

Part 3 of the Spam Act prohibits the supply, acquisition, or use of address-harvesting software.[41] It also prohibits the production of electronic address lists using address-harvesting software.[42]

Prohibiting supply of harvesting software and harvested address lists

Section 20 of the Spam Act provides that a person may not supply,[43] or offer to supply,[44] address-harvesting software,[45] or the right to use address-harvesting software. This includes harvested address lists, and the right to use those lists for other customers.[46] This applies if the supplier is an individual who is physically present in Australia, or is a body corporate or partnership that carries on business or

[39] Id s 18(9) which defines the term "unsubscribe message" as "an electronic message to the effect that the relevant electronic account-holder does not want to receive any further CEMs from or authorised by that individual or organization; or electronic message to similar effect".

[40] Id s 18(1)(e)(i) and (ii). In 2004 a regulation was implemented which provided that the use of electronic address must not require the recipient of the CEM: to use a premium service; must not cost more than the usual cost of using that kind of electronic address using the same kind of technology as was used to receive the CEM; and must not require the recipient of CEM to pay a fee or charge to the sender of the message; or a related person. See reg 3.1-3.4 of the Spam Regulations 2004 *Commonwealth of Australia Gazette* (8 April 2004). http://www.austlii.edu.au/au/legis/cht/num_reg_es/sr20042004n56202.html (date of use: 15 January 2016).

[41] Section 4 of the Spam Act defines the term "address harvesting software" as "software that is specifically designed or marketed for use for: searching the Internet for electronic addresses; and collecting, compiling, capturing or otherwise harvesting those electronic addresses".

[42] See Part 3 comprising of ss 19-22 of the Spam Act.

[43] See s 4 of the Spam Act which defines the term supply as (used in relation to goods or services) has the same meaning as in Trade Practices Act of 1974 (Australia); or (b) when used in relation to land includes transfer; or (c) when used in relation to an interest in land includes transfer."

[44] See s 20(1) of the Spam Act.

[45] Id s 4 defines the term "software" as "including a combination of software and associated data".

[46] Id s 20(1)(f) defines the term "customer" as "an individual who is physically present in Australia at the time of the supply or offer; or a body corporate or partnership that carries on business or activities in Australia at the time of the supply or offer".

activities in Australia at the time of the supply or offer.[47] Section 20 does not apply under the following circumstances: if the supplier had no reason to suspect that customers or another person intended to use the address-harvesting software or the harvested address list in connection with sending CEMs in contravention of section 16;[48] and if the supplier did not know, and could not, with reasonable diligence, have ascertained that the customer was an individual who was physically present in Australia, or a body corporate or partnership that carried on business or activities in Australia at the time of the supply or offer.[49]

Prohibiting the acquisition of address-harvesting software or address lists

Section 21 of the Spam Act prohibits a person from acquiring address harvesting software, or a right to use address-harvesting software.[50] This includes harvested address lists[51] or a right to use a harvested address list, if the person is an individual who is physically present in Australia,[52] or is a body corporate or partnership that carries on business or activities in Australia at the time of the acquisition.[53]

Subsection (1) does not apply if the person did not intend to use the address-harvesting software or the harvested address list in connection with sending CEMs in contravention of section 16.[54]

Prohibition on use of address-harvesting software and harvested address lists

Section 22 of the Spam Act prohibits an individual from using address-harvesting software or a harvested address list, if he or she is physically present in Australia at

[47] Id s 20(1)(e)(i) and (ii). Also see ACMA 'Spam address; harvesting and cold-calling prohibition' http://www.acma.gov.au/theACMA/spam-address-harvesting-and-cold-calling-prohibition (date of use: 15 January 2016).

[48] See s 20(2) of the Spam Act.

[49] Id s 20(3)(a-d).

[50] Id s 21(1).

[51] Id s 4 which defines the term "harvested address list" as "a list of electronic address; or a collection of electronic addresses; or a compilation of electronic addresses; where the production of the list, collection or compilation is to any extent, directly or indirectly attributable to the use of address harvesting software". See also ACMA 'Get smart about purchasing lists' http://www.acma.gov.au/theACMA/engage-blogs/engage-blogs/Emarketing/Get-smart-about-purchased-lists (date of use: 15 January 2016).

[52] See s 21(1)(a-e) of the Spam Act.

[53] Id s 21(1)(f).

[54] Id s 21(2).

the time of the use, or is a body corporate or partnership that carries on business or activities in Australia at the time of the use.[55] This section does not apply in relation to the use of address-harvesting software or a harvested address list if the use is not in connection with sending CEMs in contravention of section 16.[56]

Sections 16-21 also make provision for ancillary contraventions which include the following: prohibition of aiding, abetting, counseling, procuring, or inducing, whether by threats or promises; or to be in any way directly or indirectly knowingly involved in or party to, or to conspire with others to effect a contravention of subsection (1) of the sections listed above.[57] The Spam Act also makes provision for those who sent CEMs by mistake to bear the evidentiary burden of proving such mistake.[58] An individual does not contravene the sections listed above merely because he or she supplies a carriage service which enables an electronic message to be sent.[59]

The sections listed above also allow for the following exceptions: the fact that the person sending the CEM did not know, and could not with reasonable diligence have ascertained, that the message had an Australian link. [60] Sections 16-19 and 20-23 of the Spam Act have been tested in the following selected cases interpreting the Spam Act:

(e) Selected cases

Australian Communications Media Authority (ACMA) v Clarity1/Wayne Mansfield

In 2006, *Australian Communications Media Authority (ACMA) v Clarity1/Wayne Mansfield*[61] was the first case to be decided under the Spam Act. The company,

[55] Id s 22(1).

[56] Id s 22(2).

[57] Id ss 16(9); 17(5); 18(6) and (7); 20(5); 21(3); and 22(3).

[58] Id ss 16(5) and (8); 17(3) and (4); 18(5); and 20(4). Other exceptions include: the extent (if any) to which it is inconsistent with the terms of a contract or other agreement between the individual or organisation who authorised the sending of the first-message and the relevant electronic account holder if the person sent the message or caused the message to be sent by mistake.

[59] Id ss 16(10), 17(6), and 18(7).

[60] Id s 16(7)(a) and (b).

[61] See *Australian Communications and Media Authority v Clarity 1 Pty Ltd* [2006] FCA 1399 1-18 http://www.austlii.edu.au/au/cases/cth/federal_ct/2006/1399.html (date of use: 15 January 2016). Hereafter '*Clarity 1* case'; also HighBeam Research 'ACMA noose chokes off local

Clarity 1 Pty Ltd, and its director, Wayne Mansfield, were responsible for sending out in excess of 213 million UCEMs advertising their business. They operated under the trading names “Business Seminars Australia” and “Maverick Partnership”, and used both address-harvesting software and obtained harvested address lists from external parties.[62] All these acts took place around the time the Spam Act became law in 2004. The case was heard before the Perth Federal Court, and on 13 April 2006 the judge found that both Clarity 1 and Mansfield were in breach of section 16 of the Spam Act for sending UCEMs and for using harvested address lists.[63]

A defence raised in the case was that the sender relied upon inferred consent[64] having obtained the e-mail addresses before the commencement of the Spam Act, and had given the e-mail recipients the opportunity to withdraw their consent.[65] The defence was dismissed by the court which found that silence or non-response by recipients did not provide a basis for consent under the Spam Act.[66] The judge awarded a financial penalty of $ 4,5 million against Clarity 1 Pty Ltd, and $ 1 million against its managing director, Mansfield.[67] The successful prosecution of this case was credited to SpamMatters[68] for the forensic data they provided.[69]

Australian Communications and Media Authority v Atkinson

spam’ http://www.highbeam.com/doc/1G1-138418361.html (date of use: 20 January 2016); and Spamhaus ‘Australian Spam Act nails first spammer’ http://www.spamhaus.org/news/article/161/australian-spam-act-nails-first-spammer (date of use: 15 January 2016).

[62] Id *Clarity 1* case 2-3 and 9-11; and ACMA ‘Spam case studies’ http://www.acma.gov.au/theACMA/spam-case-studies (date of use: 20 January 2016).

[63] Id *Clarity 1* case 3-5. For the rules on the sending of CEMs see s 16 of the Spam Act; and for rules on address harvesting see ss 20, 21 and 22 of the Spam Act.

[64] See ACMA ‘Inferred consent and conspicuous publications’; and ACMA ‘Spam consent’ supra n 28.

[65] See ACMA ‘Spam case studies’ supra n 62.

[66] *Clarity 1* case 9-11.

[67] Ibid.

[68] SpamMatters is a reporting button which enables the user to report spam to the ACMA with a single click. See Internet Marketing Newswatch ‘ACMA launches SpamMatters’ https://imnewswatch.com/2006/05/30/acma-launches-spammatters (date of use: 15 January 2016).

[69] Ibid; also Bender supra n 26 1-24.

In the case of *Australian Communications and Media Authority v Atkinson*[70] a 26-year-old man was arrested for being behind a large-scale spam operation that sent e-mails to Internet users around the world.[71] Atkinson was pursued by the ACMA under the Spam Act after it had received more than 100 000 complaints from recipients.[72] Atkinson was fined $ 16 million by the US Federal Trade Commission after it was found that he and an American citizen, were at the center of the world's largest Internet spam operation – dubbed "Affking" – which operated by recruiting spammers from around the world.[73] Apparently the team sent billions of e-mails directing recipients to web sites advertising fake male enhancement drugs and weight-loss pills shipped from India, which they falsely claimed to have come from a licensed pharmacy in the USA.[74]

The court ordered that the respondent be restrained for a period of seven years from the date of the order from sending or causing to be sent, UCEMs from any person in Australia to anywhere, or from anywhere to persons in Australia.[75] Although Atkinson cooperated with the investigators, the court ordered him to pay a pecuniary penalty in an amount of $ 210 000 within 60 days of the order in respect of contraventions of the Spam Act.[76]

Australian Communications and Media Authority v Mobilegate Ltd

[70] *Australian Communications and Media Authority v Atkinson* [2009] FCA 1565 (22 December 2009) 1-18 http://www.austlii.edu.au/cases/cth/federal_ct/2009/1565.html (date of use: 15 January 2016). Hereafter 'the *Atkinson* case'.

[71] See Sydney Morning Herald 'World's biggest spammer' faces Brisbane court' http://www.smh.com.au/technology/security/worlds-biggest-spammer-faces-brisbane-court-20091216-kwe3.html (date of use: 20 January 2016).

[72] See *Atkinson* case supra n 70 4-7 for the facts of the case.

[73] Id 10-14; and *Federal Trade Commission v Lance Thomas Atkins* Case No 08CV5666 (2009) 1-25 http://www.ftc.gov/sites/default/files/documents/cases/2009/11/091130atkinsjudgement.pdf (date of use: 15 January 2016); and Federal Trade Commission 'Court orders Australian-based leader of international spam-network to pay $ 15.15 million: U.S. co-defendant forfeits more than $ 800 000 and faces jail time' http://www.ftc.gov/news-events/press-releases/2009/11/court-orders-australian-based-leader-international-spam-network (date of use: 15 January 2016).

[74] See the *Atkinson* case supra n 70 1-3.

[75] Id 3. See ACMA 'Penalties awarded in e-mail spam case' http://www.acma.gov.au/theACMA/acma-media-release-18720009-22december-penalties-awarded-in-email-spam-case (date of use: 15 January 2016).

[76] The respondent was also ordered to pay the applicant's costs of and incidental to the proceedings in the agreed amount of $ 15 000 within 60 days of the order. See the *Atkinson* case supra n 70 3 and 17; and ACMA 'Optus penalty for alleged breaches of Spam Act' (media release January 2009) http://www.acma.gov.au/theACMA/ acma-media-release-52009-14-january-optus-pays-penalty-for-alleged-breaches-of-spam-act (date of use: 15 January 2016).

Australian Communications and Media Authority (ACMA) v Mobilegate Ltd[77] was the first SMS spam case brought before the Federal Court. The case dealt with eight respondents – including Mobilegate Ltd and Winning Bid Pty Ltd – which had contravened the provisions of the Spam Act by sending UCEMs to mobile numbers offering chats via SMS at a cost of $ 5 per chat.[78] The ACMA alleged that the respondent was involved in a complicated scheme to obtain mobile phone numbers from members of dating web sites.[79] A penalty of $ 15.75 million was imposed on the parties involved for contravening the Spam Act.[80] The respondents were also to refrain from taking part in a variety of activities involving the use of dating web sites, the use of fictitious profiles, using photographs without permission, and contacting web site users.[81] Sections 16-21 also give rise to civil penalties which are discussed below.

7.2.3.3 Civil penalties

Part 4 of the Spam Act deals with a number of issues related to civil penalties.[82] Section 24 deals with pecuniary penalties for contravention of the Act's civil penalty provisions. It provides that a Federal Court[83] may order an individual to pay a pecuniary penalty which the court deems appropriate in respect of each contravention.[84] In determining the pecuniary penalty, the court must have regard to

[77] *Australian Communications and Media Authority v Mobilegate Ltd* [2010] FCA 1197 (5 November 2010) 1-35 http://www.austlii.edu.au/au/cases/cth/FCA/2010/1197.html (date of use: 15 January 2016). Hereafter '*Mobilegate* case'.

[78] Id 11-22 for the facts of this case. Other cases dealing with SMS spam include those on e-mails originating in Australia encouraging recipients to join a pyramid scheme; and SMS spam originating overseas providing racing tips software advertising. See ACMA 'Million dollar penalties issued in first SMS spam case' (August 2009) http://www.acma.gov.au/theAcma/acma-media-release-1512009-23-october-million-dollar-penalties-issued-in-first-sms-spam-case (date of use: 15 January 2016) and ACMA 'Federal Court finds Brisbane man breached Spam Act' (December 2010) http://www.acma.gov.au/theACMA/federal-court-finds-brisbane-man-breached-spam-act (date of use: 15 January 2016).

[79] See *Mobilegate* case supra n 77 11-22.

[80] Ibid.

[81] Ibid. Also ACMA 'ACMA obtains interlocutory orders in SMS spam case' http://www.acma.gov.au/theACMA/acma-obtains-interlocutory-orders-in-sms-spam-case (date of use: January 2016).

[82] In terms of s 4 of the Spam Act civil penalty provisions cover the following: s 16(1), (6) and (9); s 17(1) and (5); s 18(1) and (6); s 20(1) and (5); s 21(1) and (3); s 22(1) and (3); and a provision in the regulations declared to be civil-penalty provision in accordance with s 45(2)(c).

[83] Section 4 of the Spam Act defines the 'Federal court' as the Federal court of Australia.

[84] Id s 24(1).

all relevant issues including:[85] the nature and the extent of the contravention; the nature and extent of any loss or damage suffered as a result of the contravention;[86] the circumstances in which the contravention took place;[87] and whether the person has previously been found to have engaged in any similar conduct.[88] If the court considers it appropriate to do so, it may also take account of whether the person has previously been found to have engaged in any similar conduct by a court in a foreign country.[89]

Section 25 provides for a maximum penalty payable by a person in respect of a contravention of the Spam Act which attracts a civil penalty depending on whether that person has a prior conviction[90] in relation to the civil-penalty provision.[91] The maximum penalty is payable by different people or institutions such as a body corporate with[92] or without a prior record,[93] or a person other than a body corporate with[94] or without a prior record.[95]

[85] Id s 24(2).

[86] Ibid.

[87] Ibid.

[88] Ibid.

[89] Ibid.

[90] "Prior record" means "an order under s 24(1) against a person in respect of a contravention of a particular civil penalty provision; and that the first occasion for the purposes of determining the penalty payable under s 24(1) by the person in respect of a contravention of the civil penalty provision that occurs after the first day, the person has a prior record in relation to the civil penalty provision". Id s 25(2).

[91] Id s 25(1).

[92] Id s 25(5) which states the different kinds of penalty ranging from 500 penalty units to 5 000 and 10 000 penalty units for having contravened the civil penalty provision two or more times in a day. See Victoria Legal Aid 'Penalty units' https://www.legalaid.vic.gov.au/find-legal-answers/fines-and-infringements/penalty-units (date of use: 15 January 2016).

[93] Id 25(3) which provides that: "if there is no prior record then the civil penalty provision must not exceed 100 penalty units (if it relates to s 16(1), (6) or (9)); and in any other case 50 penalty units; in case the body corporate has committed two or more contraventions 2 000 penalty units, or in any other case 1 000 penalty units are payable".

[94] Id s 25(6)(b). In this instance the Act provides that: "if there is a contravention of a civil penalty in terms of s 16(1), (6) of (9) the penalty must not exceed 100 penalty units, or in any other case 50 penalty units. And if the Federal court finds that the person committed two or more contraventions on a particular day, then the total of the penalties payable under subsection 24(1) must not exceed 2 000 penalty units in the case of subsections 16(1), (6) or (9), or in any other case 1 000 penalty units".

[95] Id s 25(4)(a) and (b). This section provides that: "if there is a contravention of a civil penalty in terms of s 16(1), (6) or (9) the penalty must not exceed 20 penalty units, or in any other case 10 penalty units. And if the Federal court finds that the person committed two or more contraventions on a particular day, then the total of the penalties payable in terms of subsection 24(1) must not exceed 400 penalty units in the case of subsections 16(1), (6) or (9), or 200 penalty units in any other case".

Section 26 provides that the ACA may institute proceedings in a Federal Court on behalf of the Commonwealth for the recovery of a pecuniary penalty referred to in section 24 above.[96] The proceedings in subsection 1 may be commenced within six years after the contravention.[97] The Federal Court may direct that two or more proceedings under subsection (1) be heard together.[98] In terms of the Spam Act, criminal proceedings may not be brought for contravention of civil penalties.[99]

7.2.3.4 Ancillary orders

Section 28 provides for ancillary orders in the form of compensation and recovery of financial benefits.

(a) Compensation

If the Federal Court finds that a person has contravened one or more civil-penalty provision under section 26,[100] and it is satisfied that another person has suffered loss or damage as a result of any or all of those contraventions, it may, on application by the ACA or the victim, issue an order it considers appropriate directing the perpetrator to compensate the victim.[101]

In determining whether the person has suffered loss or damage as a result of one or more contravention by another person in relation to sending of one or more CEMs, and in assessing the amount of the compensation payable, the court may have regard to the extent to which any expenses incurred by the victim can be attributed to dealing with the message.[102] The effect of dealing with the messages on the victim's ability depends on the business's ability to carry on business or other activities.[103]

[96] Id s 26(1).
[97] Id s 26(2).
[98] Id s 26(3).
[99] Id s 27.
[100] Id s 28(1)(a).
[101] Id s 28(1)(b).
[102] Id s 28(2).
[103] Ibid. The Federal court may make an order in subsection (1) whether or not it makes an order under s 24. An application under subsection (1) may be made at any time within 6 years after the contravention concerned (id s 28(3) and (4)).

(b) Recovery of financial benefit

Proceedings under section 26 may be instituted if the Federal Court finds that a person has contravened one or more civil-penalty provision and it is satisfied that the person has obtained (whether directly or indirectly) a financial benefit that is reasonably attributable to any or all of the contraventions.[104] The court may, on application by the ACA, issue an order directing the offender to pay to the Commonwealth an amount up to the amount of the financial benefit.[105] An application under subsection (1) may be made at any time within six years after the contravention occurred.[106]

7.2.3.5 Injunctions

The issue of injunctions is dealt with in Part 5 of the Spam Act.[107] Injunctions come in the following forms: restraining injunctions; performance injunctions; and interim injunctions. A restraining injunction applies if a person has engaged in, or is engaging or proposing to engage in, any conduct in contravention of a civil-penalty provision.[108] The Federal Court may, on application by the ACA, grant an injunction restraining the person from engaging in such conduct.[109] If, in the court's opinion, it is desirable to do so, the injunction may require the person to do something.[110] There are also certain limits on the grant of restraining injunctions.[111] The performance

[104] Id s 29(1)(a).

[105] The Federal court may make an order under subsection (1) whether or not it makes an order under s 24. Id s 29(1)(b) and (2).

[106] Id s 29(3).

[107] Id ss 31-36.

[108] Id s 32(1).

[109] Id s 32(1)(a).

[110] Id s 32(1)(b).

[111] Id s 35(1) deals with these issues and gives the Federal Court the power to grant injunction restraining a person from engaging in conduct of a particular kind. and may be exercised: "if the court is satisfied that the person has engaged in conduct of that kind whether or not it appears to the court that the person intends to engage again or to continue to engage in conduct of that kind; or if it appears to the court that if an injunction is not granted it is likely that the person will engage in conduct of that kind, whether or not there is an imminent danger of substantial damage to any person if the person engages in conduct of that kind". Section 35(2) gives the Federal court the power to grant an injunction requiring a person to do an act or thing: "if the court is satisfied that the person has refused or failed to do that act or thing, whether or not it appears to the court that the person intends to refuse or fail to perform again or to continue to refuse or fail to do that act or thing; or if it appears to the court that if an injunction is not granted it is likely that the person will refuse or fail to do that act or thing whether or not the person has previously refused or failed to do that act or thing and whether or not there is an

injunction applies in cases where a person has initially refused or failed to perform an act, and that refusal or failure would be a contravention of a civil-penalty provision. The Federal Court may on the application of the ACA, grant an injunction requiring that particular person to perform the act.[112]

If an application is made to the Federal Court for an injunction under section 32, before considering the application the court may grant an interim injunction restraining the person from engaging in conduct of a kind referred to in section 32.[113] The Federal Court may not require an applicant to give any undertakings as to damages when applying for an interim injunction under section 32.[114] It may also discharge or vary an injunction granted under Part 5.[115] The powers conferred on the Federal Court under Part 5 are additional to, and not in place of, any other powers of the court – whether conferred by the Act or otherwise.[116] The Spam Act also makes provision for miscellaneous provisions in Part 7.[117]

7.2.3.6 Enforcement of the Spam Act

(a) Introduction

The Spam Act was enforced by the ACA until 2005 when the ACMA took over this function. The goal of the ACMA is to promote confidence in electronic messaging as a form of commercial communication.[118] The compliance and enforcement approach

imminent danger of substantial damage to any person if the person refuses or fails to do that act or thing".

[112] Id s 32(2)(a) and (b) of the Spam Act.

[113] Id s 33(1).

[114] Id s 33(2).

[115] Id s 34.

[116] Id s 36.

[117] Id s 43-47 where the following miscellaneous provisions are contained: "the Act is not intended to exclude or limit the operation of a law of a state or territory to the extent that the law is capable of operating concurrently with this Act; the Act does not apply to the extent (if any) that it would infringe any constitutional doctrine of implied freedom of political communication; the regulations may make provision for and in relation to giving effect to an international convention that deals with either or both of the CEMs, and address harvesting software; the Minister must conduct a review of the operation of this Act and others before the end of two years after commencement of the Act; and the Governor-General may make regulations prescribing matters required or permitted to be prescribed by the Spam Act; and necessary or convenient to be prescribed for carrying out or giving effect to the Act".

[118] See ACMA 'Introduction to the ACMA' http://acma.gov.au/theACMA/About/Corporate/Authority/introduction-to-the-acma (date of use: 23 March 2017).

to the Spam Act establishes how the ACMA operates to minimise spam being sent from Australia, as well as the impact of spam on Australian nationals.[119] The ACMA relies on market intelligence, internal engagement, education, and industry partnerships to assist and support the compliance and enforcement approach.[120]

The Spam Act provides enforcement options and the ACMA determines appropriate action on a case-by-case basis.[121] Enforcement actions are offered by the ACMA at any time, and provide an opportunity for a business or individual to formalise its commitment to comply with the Spam Act.[122] The ACMA will consider the following factors when determining the appropriate outcome to an investigation: the impact of the message on members of the public; the number of warnings the sender has received;[123] and the regularity and severity of the volume of the messages.[124] Other considerations are whether the sender has cooperated with the ACMA, and whether the messages involved deceptive practices.[125] In most circumstances, the ACMA will take administrative action which is likely to conclude in an informal warning; enforceable undertakings;[126] or an infringement notice.[127]

(b) Enforceable undertakings

[119] Ibid.

[120] Ibid.

[121] See ACMA 'Spam and legislation enforcement' http://www.acma.gov.au/Industry/Marketers/Anti-Spam/Ensuring-you-dont-spam/spam-legislation-enforcement-ensuring-you-dont-spam-i-acma (date of use: 23 March 2017).

[122] Ibid.

[123] Ibid.

[124] Ibid.

[125] Ibid.

[126] See ACMA 'Enforceable undertakings: guidelines for the use of enforceable (Telecommunication Obligations)' March 2006 1-8 http://www.acma.gov.au/~/media/Legal% 20 Services/Advice/pdf/Enforceable%20undertakings%20Guidelines%20Guidelines%20for%20the%20use%20of%20enforceable%20undertakings%20Telecommunications%20Obligations.pdf (date of use: 15 January 2016).

[127] For a discussion on infringement notices see ACMA 'Regulation Guide: No 5 Infringement Notices' (September 2011) 1-6 http://www.acma.gov.au/~/media/Legal%20Services/Advice/pdf/Regulatory%20guide%20No%205%20Infringement%20notices.PDF (date of use: 15 January 2016); and ACMA 'Cellarmaster Wines penalised' (media release May 2013) http://www.acma.gov.au/Industry/Marketers/Anti-Spam/Ensuring-you-dont-spam/cellarmaster-wines-penalised-for-spam-act-breaches (date of use: 20 January 2016). This case involved marketing-e-mail messages being sent without an opt-out facility, while others were sent to customers who had previously chosen to opt-out of such promotions and thus contravened s 16-18 of the Spam Act. The business paid $ 111 000 in infringement notices following an investigation by the ACMA.

The issue of enforceable undertakings is dealt with in Part 6 of the Spam Act which covers CEMs and address-harvesting software.[128] The ACMA may accept a written undertaking given by a person for the purposes of contravening specific provisions in the Spam Act.[129] The person may, with the consent of the ACMA, withdraw or vary the undertaking at any time.[130] If the ACMA considers that an individual who has been granted an undertaking under section 38 has breached any of the terms of the undertaking, it may apply to the Federal Court for an order.[131]

An enforceable undertaking is a flexible tool in that it can enable past misconduct to be rectified and shape future behavior, including introducing preventative measures where there is a risk of breach rather than an actual breach.[132] The advantages of enforceable undertakings are noted as: saving time, costs, and court resources required for litigation;[133] and also that the party who gives the undertaking takes responsibility for its own organisational and behavioural change.[134] In order to allow for compromise, both parties can contribute to structuring the compliance action, and also allow flexibility and the opportunity for behavioural change.[135] Enforceable undertakings also encourage learning and ensure that the regulated entity's process of compliance is on-going.[136]

The assessment of compensation for breach of undertaking is determined when the Federal Court finds that a person has breached a term of an undertaking relating to the sending of CEMs.[137] The court will have regard to the following factors when determining whether the breach has caused another person to suffer loss and damages, and also when assessing the amount of compensation payable, including

[128] See ss 37-40 of the Spam Act.

[129] Id s 38(1).

[130] Id s 38(2).

[131] Id s 39(1) and (2). These orders include: "an order directing the person to comply with the term of the undertaking; an order directing the person to pay to the Commonwealth any financial benefit that the person has obtained directly or indirectly and that is reasonably attributable to the breach; any order that the court considers appropriate directing the person to compensate any other person who has suffered loss or damage as a result of the breach; and any other order that the court considers appropriate".

[132] See ACMA 'Enforceable undertakings: guidelines for the use of enforceable (Telecommunication Obligations)' supra 126 1-8.

[133] Ibid.

[134] Ibid.

[135] Ibid.

[136] Ibid.

[137] Id s 40.

the extent to which any expenses incurred by the victim are attributable to dealing with the messages[138]

Examples of enforceable undertakings by companies in compliance with the provisions of Spam Act

Since the coming into operation of the Spam Act, a number of enforceable undertakings have been met by businesses that had contravened some provisions in the Act.[139] The format of these undertakings is largely similar and makes provision for definitions; the name of the infringing company; the infringement of a particular provision in the Spam Act; and a background to the charges facing the company.[140] Upon investigation by the ACMA, the company may undertake to perform certain duties which include making payments of a specified amount for previous CEMs sent without consent, and for conduct which will ensure that no further CEMs are sent.[141] The company must also review its e-marketing activities to ensure compliance with the Spam Act,[142] offer its employees training,[143] and engage in quality assurance.[144]

[138] Id s 40(2). Other factors include: "the effect of dealing with the messages on the victim's ability to carry on business or other activities; any damage to the reputation of the victim's business that is attributable to dealing with the messages; any loss of business opportunities suffered by the victim as a result of dealing with the messages; and any other matters that the court considers relevant".

[139] These include enforceable undertakings on the following sections s 16-18 dealing with the sending of CEMs without consent, or without an identifying label and facilitation of the unsubscribe link; and s 20-22 on address harvesting provisions. See ACMA 'The ACMA's enforceable undertakings' http://www.acma.gov.au/theACMA/About/The-ACMA-story/Regulating/the-acmas-enforceable-undertakings (date of use: 20 January 2016) and ACMA 'Enforcement action archives' http://www.acma.gov.au/theACMA/acma-enforcement-action-archives (date of use: 15 January 2016).

[140] See *JER Pty Ltd* (CAN 107 555 475 19 October 2011) 1-4 http://www.acma.gov.au/webwr/_assets/main/lib310480/urban_agent-eu_s38_spam_act.pdf (date of use: 20 January 2016).

[141] Payments usually differ depending on the undertaking.

[142] Companies either conduct these reviews themselves or employ independent consultants to review such activities. A report is produced identifying the deficiencies and recommending improvements to policies and procedures to ensure the Spam Act compliance. An independent consultant will also recommend the frequency and scope of audits (including when and how often CEM campaigns or percentages of campaigns should be audited). See *Nokia Corporation* (media release 3 January 2012) 3-4 http://www.acma.gov.au/webwr/assets/main/lib310480/nokia-eu_s38_spam_act-3jan2012.pdf (date of use: 20 January 2016).

[143] Usually companies undertake to develop and submit to ACMA for approval within a specified period, a detailed written copy of its training program, which will provide minimum training on the requirements of all provisions of the Spam Act. The training is usually offered to the employees, licensees, contractors, and affiliates who are involved in any activity. Once the training is completed a written confirmation should be sent to ACMA. Training is also offered to new employees who are involved in any activity in connection with that business or is likely to be responsible for the sending of CEMs within a specified period. See *EventsHQ Pty Ltd* (ACN

Undertakings in terms of the Spam Act apply for a specified period.[145] Companies also acknowledge their involvement in contravening some provisions in the Spam Act.[146]

Club Retail Pty Ltd

118 063 666) 3-4 http://www.acma.gov.au/webwr/_assets/main/lib310480/eventshq-s38_spam_act-eu.pdf (date of use: 20 January 2016). Hereafter '*EventsHQ* case'.

[144] This includes the respective company undertaking to review and submit to ACMA for approval a detailed written copy of its relevant quality assurance processes to ensure that the sending of CEMs by that particular company is complaint with the sections infringed. This quality assurance includes a requirement that the company in question comply with a particular section, for example: that the company ensure that each relevant electronic account holder within a list of proposed recipients of CEMs has consented to the receipt of the CEM (in terms of s 16); and in terms of s 17, by reviewing the proposed message to ensure that the content of the message does not contain accurate information about how the recipient of the message could readily identify and contact the organisation which authorised the message; and s 18 by reviewing the proposed message to ensure that the content of the message contains a functional unsubscribe facility. See *Virgin Blue Pty Limited* (ACN 090 670 965 26 February 2010) 1-8 http://www.acma.gov.au/webwr/_assets/main/lib310480/virgin_blue_s38_spam_act-enforceable_undertaking.pdf (date of use: 20 January 2016) and *Best Buy Australia Pty Ltd* (ACN 122 464 799 media release 24 February 2010) 1-8 http://www.acma.gov.au/~/media/Unsolicited%20Communications%20Compliance/Enforceable%20understanding/pdf/EU%20Best%20Buy%20Australia%20PL%20August%202010%20Spam%20Act%202003.PDF (date of use: 20 January 2016).

[145] The expiry dates of such undertakings differ from case to case. In some instances the undertaking remains in force indefinitely unless otherwise agreed to in writing between ACMA and the undertaking party or unless varied or terminated by order of the Federal court in Australia. See the following undertakings: *Qidi Enterprises Pty Ltd* (ABN 35097220114 media release 20 January 2006) 3 http://www.acma.gov.au/webwr/_assets/main/lib310480/p_liang_qidi_enterprises-ast_enforc_utaking.pdf (date of use: 20 January 2016); *Oxygen8 Communications Australia Pty Ltd* (ACN 111 902 982 media release 15 December 2008) 3 http://www.acma.gov.au/webwr/_assets/main/lib310480/oxygen8_s38_spam_act.pdf (date of use: 20 January 2016); and *AustraliaSMS Pty Ltd* (ABN 30 100 396 138 and ACN 100 396 138 media release 21 July 2005) 3 http://www.acma.gov.au/webwr/_assets/main/lib310480/aust/sms-boulos-ast_enforc_utaking.pdf (date of use: 20 January 2016). Others have specified periods of 36 months: see *Funmobile Australia Pty Ltd* (ACN 114 489 600 media release 19 January 2010) 5 http://www.acma.gov.au/webwr/_assets/main/lib310480/funmobile_s38_spam_act_eu.pdf (date of use: 20 January 2016); 12 months: see *New Dialogue Pty Limited* (ACN 111 086 938 media release 29 September 2009) 6 http://www.acma.gov.au/webwr/_assets/main/lib310480/new_dialogue_s38_spam_act_eu.pdf (date of use: 20 January 2016).

[146] These acknowledgements are by companies that have undertaken to perform an act. Usually these companies acknowledge that ACMA may make an undertaking available for public inspection; issue a media release on the acceptance of the undertaking; and also that the undertaking does not derogate from any rights and remedies available to any other person arising from the conduct described in the undertaking. See the following undertakings: *Tiger Airways Holdings Limited* (ACN 124 369 008 media release 22 October 2012) 1-9 http://www.acma.gov.au/webwr/_assets/main/lib310480/tiger_airways-%20eu_s38_spam_act-22oct2012.pdf (date of use: 20 January 2016); and *Big Mobile Pty Ltd* (ACN 119 902 966 media release 29 September 2009) 1-6 http://www.acma.gov.au/webwr/_assets/main/lib310480/big_mobile_s38_spam_act_eu.pdf (date of use: 20 January 2016).

In *Club Retail Pty Ltd*[147] the ACMA commenced an investigation in January 2015 against Club Retail (an incorporated entity offering daily online deals) for contravening section 16 of the Spam Act. Club Retail had sent 294 CEMs without the consent of the recipients between June and December 2014. In February 2015 the ACMA wrote to Club Retail outlining its preliminary views and providing it with an opportunity to comment. In response, Club Retail undertook to establish a double opt-in process for obtaining consent from account holders of electronic addresses before sending CEMs to those addresses.[148] It also undertook to desist from sending CEMs to any account holders who had not consented to receive such messages using the double opt-in process, unless the relevant electronic account holder had purchased an item from Club Retail.[149]

Club Retail further accepted that the ACMA could issue a media release on execution of this undertaking by referring to its terms, which included that ACMA could publish the undertaking or make it available for public inspection, and could also refer to the undertaking publicly from time to time.[150]

EventsHQ Pty Ltd

EventsHQ Pty Ltd[151] is a company incorporated in New South Wales which carried on business in Australia as a provider of poker events to pubs and clubs under the NPL brand.[152] In 2011 there was an investigation into the company for having contravened sections 16,[153] 17,[154] and 18 of the Spam Act.[155] The company paid $

[147] See *Club Retail Pty Ltd* (ACN 165 324 881 media release 2015) 1-3. Hereafter '*Club Retail*'.

[148] Id 2. This double opt-in process requires the electronic account holder to confirm consent to the receipt of CEMs using the electronic address to which CEMs will be sent. See ACMA 'Double opt-in helps marketers' double check' http://www.acma.gov.au/Industry/Marketers/Anti-Spam/Ensuring-you-dont-spam/double-opt-in-helps-marketers-double-check-1 (date of use: 20 January 2016); and ACMA 'The ACMA accepts enforceable undertaking from Alex Shehata' http://www.acma.gov.au/theACMA/the-acma-accepts-enforceable-undertaking-from-alex-shehata (date of use: 20 January 2016).

[149] Id 2. Confirmation was also received from relevant electronic account holders that consented to the receipt of CEMs from Club Retail in response to an electronic message sent to them using electronic address to which CEMs had previously been sent seeking confirmation of their consent to continue receiving CEMs from Club Retail; and which includes no content that offers to supply advertise or promote Club Retail.

[150] Id 2-3.

[151] See *EventsHQ* case supra n 143 1-6.

[152] Id 2.

[153] They contravened this section by sending or causing to be sent 91 CEMs without consent of the recipient.

22 000 for the CEMs which were subject to the investigation.[156] It also undertook to develop and submit to the ACMA for approval, a written copy of its training program which would (as a minimum) provide training on the requirements of all provisions of the Spam Act.[157]

Nokia Corporation

Nokia Corporation[158] is a company incorporated in Finland with customers throughout the world, including Australia. Nokia sent CEMs to its Australian customers from outside of Australia. Upon investigation, the ACMA was concerned that Nokia had contravened sections 16, 17 and 18 of the Spam Act. Nokia acknowledged that this was in fact the case, and undertook to pay $ 55 000 in settlement of the issues relating to the CEMs which the ACMA had investigated.[159]

Apart from enforcement undertakings, the Spam Act also makes use of formal warnings which are outlined below.

(c) Formal warnings

Section 41 of the Spam Act authorises the ACMA to issue formal warnings to a person or company that contravenes the provisions in the Act, including sections 16(1)[160] and 18.[161] These warnings are issued to those companies that are in

[154] The company contravened this section by sending or causing to be sent 62 967 CEMs without clear and accurate identification of who authorised the sending of the message.

[155] This company contravened the section by sending or causing to be sent 110 330 CEMs without contact details of the authoriser of the CEMs.

[156] Id 3.

[157] Ibid.

[158] *Nokia Corporation* supra n 142 1-6.

[159] Id 3.

[160] These formal warning include but are not limited to the following: *Vadkho Pty Ltd* (ACN 138 809 917 media release 22 April 2015) 1-2 http://www.acma.gov.au/Citizen/Take-action/Complaints/Spam-complaints/spam-enforcement-actions (date of use: 20 January 2016). An investigation commenced in June 2014 by the ACMA against Vadkho (which traded as GoDeals) for contravening s 16(1) by sending 197 CEMs that had an Australian link. These messages were sent for the purpose of offering to supply GoDeals' goods or services, which resulted in the messages being CEMs; also *IGEA Life Sciences Pty Limited* (ACN 125 930 878 media release 30 June 2014) 1-2 http://www.acma.gov.au/~/media/Unsolicited%20Communications%20Compliance/Formal%20warning/PDF/20140630%20%20IGEA%20Life%20Sciences%20Pty%20Limited%20%20Formal%20warning%20pdf.PDF (date of use: 20 January 2016). This formal warning entailed an

contravention of the Spam Act as a result of having sent messages without consent, and also to those who have violated the Act by failing to provide information on how a recipient could opt-out of the unwanted CEM.

7.2.4 Commentary on the Spam Act

7.2.4.1 Background

In what follows a commentary on the Spam Act and how it has been perceived by different stakeholders is highlighted. First the discussion is on the benefits of the Act, followed by the criticisms levelled at the Act and finally a conclusion.

7.2.4.2 Benefits of the Spam Act

investigation into IGEA which had allegedly contravened s 16 of the Spam Act. The ACMA had received complaints from consumers who had received CEMs from IGEA Life Sciences. It was determined that IGEA Life Sciences had indeed sent or cause to be sent electronic messages between the period of 17 July 2013 and 11 October 2013; *Wailea Australia Pty Ltd* (ACN 155 959229 media release 07 October 2013) 1-2 http://www.acma.gov.au/~/media/Unsolicited%20Communications%20Compliance/Formal%20warning/ACRIS%20Svces%20ss161%20Formal%20warning%20Spam%20Act%20pdf.pdf (date of use: 20 January 2016). Wailea Pty Ltd trading as ACRIS Services was found to have sent 17 electronic messages in contravention of s 16 of the Spam Act between 1 February 2013 and 27 May 2013; and *DND Media Pty Ltd* (ACN 151 096 285 media release 05 September 2013) 1-2 http://www.acma.gov.au/~/media/Unsolicited%20Communications%20Compliance/Formal%20warning/DND%20Media%20s41%20Spam%20Act%20Formal%20Warning%20%20pdf.pdf (date of use: 20 January 2016). DND was found to have contravened s 16(1) of the Spam Act by sending or causing to be sent 30 electronic messages between 5 February 2013 and 2 May 2013.

[161] Examples of formal warnings issued include: *McDonald's Australia Limited* (ACN 008 496 928 media release 18 December 2012) 1-2 http://www.acma.gov.au/Industry/Marketers/Anti-Spam/Ensuring-you-dont-spam/mr-992012-acma-warns-mcdonalds-for-send-to-friends-marketing (date of use: 20 January 2016). This formal warning involved an investigation by the ACMA that found e-mails to have been sent using the "send-to-friend" facility (which promoted games and activities) which were sent to friends of users without ensuring the friends' consent. The messages also did not have an unsubscribe facility as required by Spam Act. McDonalds later removed the "send-to-friend" facility from the happy meal web site and has given assurance as to its future e-marketing activities; *Penta Group Pty Ltd* (ACN 122757519 media release 2014) 1-2 http://www.acma.gov.au/theACMA/penta-group-pty-ltd (date of use: 20 January 2016). Penta Group was said to have contravened s 18(1) of the Spam Act by sending or causing to be sent 7 CEMs which had an Australian link and were not designated CEMs without the consent of the relevant account holders; and *Global Billing Solutions Pty Ltd* (ACN 135 029 748 media release 23 March 2012) 1-2 http://www.acma.gov.au/webwr/_assets/main/lib410040/global_billing_solutions-formal_warning_spam_act.pdf (date of use: 20 January 2016). This formal warning dealt with the contravention of s 18 of Spam Act by the company Global Billing Solutions. As a result of the investigation it was found that this company had sent four electronic messages with an Australian link between 1 July 2010 and 6 August 2010 users without consent. See ACMA 'Formal warning index' http://www.acma.gov.au/theACMA/formal-warnings (date of use: 20 January 2016).

Three months after its inception, the Spam Act was hailed by the ACA as an effective deterrent to spammers.[162] The ACA claimed that after the Act came into operation, complaints about spammers had supposedly stopped.[163] Those in favour of the Spam Act noted that while the Act is not a “silver bullet”, it is however a key element in the government’s approach to spam.[164] In 2006 it was reported that the Spam Act had proven to be effective against professional spammers and had driven most of them out of the country.[165] The Spam Act was also hailed as having imposed limits – accepted by both the business community and consumers – on e-marketing by responsible Australian businesses.[166] It was further noted that Australia has strong legislation to regulate spam by limiting unsolicited e-marketing, which has proved effective in reducing the amount of spam created within its borders.[167]

7.2.4.3 Criticisms of the Spam Act

Immediately after its enactment, it was reported that the Spam Act came under heavy criticism from opposition politicians who believed that “a wide range of the exemptions in the law favoured certain interest groups”.[168] These exemptions relate to the fact that only commercial spam is outlawed, whereas political parties, religious organisations, and charities can still use spam to reach people.[169] This, according to some, “makes it difficult to understand why, assuming that lawmakers considered the existing legislation relating to the control of marketing as inadequate, they still chose not to amend it to increase its efficacy”.[170] It has also been acknowledged that the Spam Act is not a cure for all spam-related matters.[171] The Act has furthermore been referred to as “clumsy and flawed” by the Australian Democrats.[172] Holmes notes

[162] FindLaw Australia ‘Government Spam Act closes down major spammers’ http://www.findlaw.com.au/news/4662/government-spam-act-closes-down-major-spammers.aspx (date of use: 15 January 2016).

[163] Ibid.

[164] See South China Morning Post ‘Australian anti-spam law sparks fierce criticism’ http://www.scmp.com/article/437282/australian-anti-spam-law-sparks-fierce-criticism (date of use: 15 January 2016).

[165] See ACMA ‘Submission to Spam Act Review: ACMA’ supra n 1 28.

[166] Ibid.

[167] See Manwaring (2009) *Computers and Law* 8.

[168] Ibid.

[169] Ibid. This is consistent with most anti-spam laws including those of the USA above.

[170] Ibid.

[171] Ibid; also South China Morning Post ‘Australian anti-spam law sparks fierce criticism’ supra n 164.

[172] Ibid.

that the Spam Act is voluminous and difficult to understand fully, which might be the reason why there are many accompanying documents that, in particular, explain how businesses can continue their use of the Internet for marketing.[173] Holmes argues for an improvement to the current laws regulating spam as opposed to the introduction of a new legislation which is specific to the Internet.[174] The fact that enforcement of the new anti-spam law depends on encouragement and compliance[175] does not mean that it will put a stop to unsolicited e-mails getting through to home computers, even if the Act sends the message that that practice is unacceptable.[176] Kent is of the view that it is unlikely that the Spam Act will have a meaningful impact on reducing the amount of spam transmitted through the Internet.[177]

Further, by trying to regulate the senders of spam based on their geographic location, the Australian government is said to be "attempting to solve the digital problem by using an outmoded analogue concept of Australian sovereignty".[178] Some are of the opinion that domestic legislation alone is insufficient to eliminate spam, or even to reduce it to an acceptable level, and further that enforcement efforts under international law do not resolve the problems arising from conflicting obligations in a cross-jurisdictional context.[179]

Bender notes that "the problem with relying on domestic legislation alone (even coupled with soft measures such as education), and any unilateral, exclusively legislative approach taken by other national governments, is limiting in that the spam problem is global with the vast majority of spam originating from outside of Australia".[180] Another shortcoming in the Spam Act is noted as: its failure to provide grounds for civil action by individuals or corporations against spammers, so making the ACMA the only party with standing.[181] The Act also fails to render ISPs

[173] See Holmes (2005) 38 *The Profession* (2005) 87.

[174] Id 86.

[175] Ibid.

[176] See Walker F 'Even the new anti-spam laws won't stop those pesky emails' http://www.spamstop.com.au/spam-stop-articles/2004/2/7/even-new-antispam-laws-wont-stop-those-pesky-emails (date of use: 15 January 2016).

[177] See Kent (2004) 76/4 *Australian Quarterly* 4.

[178] Id 5.

[179] See Manwaring supra n 167 8.

[180] See Bender supra n 26 7.

[181] Id 10. This is also consistent with the USA's position in Chapter 6 par 6.4.3.3 above.

accountable for reducing spam levels, seeing that most of the spam that reaches consumers comes via ISPs.[182]

7.2.5 Conclusion

Australia, like the USA above, has taken the first step in implementing an anti-spam Act. The Spam Act embodies most, if not all, the requirements set for anti-spam legislation: its provisions are clear and relevant penalties are prescribed. As the discussion above shows, Australia's Spam Act has been effective in combating spam especially within its borders. Between the years 2004 and 2005 the ACMA received more than 200 000 reports of spam on its hotline and web site.[183] These were, in the main, recorded as coming from offshore sites, or were classified as "slip-ups" which did not require further investigation.[184]

In 2015 the spam statistics for Australia revealed that the reports and complaints received per month had increased from those in 2014 statistics– almost 30 000 reports were received in that year.[185] By January 2016 the statistics had increased to over 30 000, while some months stood at close to 40 000 or more.[186] These statistics are an indication that the undertakings and formal warnings are effective in minimising spam in Australia.

The variety of enforcement actions and the encouragement of voluntary compliance are a plausible attempt to combat spam in that they also cater for small and medium-sized businesses which might not have the income to pay heavy penalties. However, by complying with those undertakings companies can also learn how to market their businesses without contravening the provisions of the Spam Act. While Australia might have minimised its spam intake in the country, it is still confronted with spam at a global level, a task they have addressed in the MoUs outlined below. In the

[182] Id 12.

[183] See HighBeam Research 'ACMA noose chokes off local spam' supra n 61.

[184] Ibid.

[185] See ACMA 'Spam statistics: January 2015' http://www.acma.gov.au/theACMA/ACMAi/investigation-reports/Statistics/spam-statistics (date of use: 15 January 2016).

[186] See ACMA 'Spam statistics: January 2016' http://www.acma.gov.au/theACMA/ACMAi/investigation-reports/Statistics/spam-statistics (date of use: 15 January 2016).

discussion below the remaining measures are highlighted to judge how effective Australia has been in combating spam.

7.3 Other multi-faceted measures to combat spam

Section 42 of the Spam Act provides the following in addition to ACMAs functions: to conduct and/or coordinate community education programs on UCEMs; to address software harvesting in consultation with relevant industry and consumer groups and government agencies; to conduct and/or commission research into these measures; and to liaise with regulatory and other relevant bodies on cooperative arrangements for the prohibition or regulation of spam matters.

7.3.1 Consumer education and awareness

In June 2009 the unsolicited communications survey undertaken on behalf of the ACMA found that 78 per cent of respondents had heard of the term “spam”, and that most respondents usually deleted spam without opening it.[187] In 2010 the ACMA launched a new reporting tool, the “spam SMS” which provided Australians with a quick and easy way to report SMS spam by forwarding messages received to a specific number.[188]

The ACMA also installed a number of programs to minimise cyber threats, most notably the “Spam Intelligence Database”.[189] Consumers were urged to report spam via this web site (where e-mail addresses are provided for the queries). However, consumers were also cautioned, before reporting a complaint, to note that the Spam

[187] See ACMA ‘Spam education and awareness’ http://acma.gov.au/Citizens/Complaints/Internet-complaints/Spam-complaints/spam-educationandawareness (date of use: 15 January 2016). In 2013 a follow-up survey found similar results with 87% of respondents deleting e-mail spam without opening it.

[188] See Tay L ‘ACMA launches spam SMS reporting tool’ http://www.itnews.com.au/News/214731,acma-launces-spam-sms-reporting-tool.aspx (date of use: 20 January 2016). “These spam complaints are related to scam activities including messages about fake lottery wins or pleas to transfer large sums of money. The Regulator reported that already in 2008/2009 there had been a 71% increase in SMS spam complaints, and a 12% increase in the first eleven months of 2009/2010. Consumers were more sensitive to SMS spam, and that the character of SMS limit created problems in providing accurate sender information and unsubscribe instructions. Complaints were often complex, and malicious use of SMS messages indicated that over 60% of SMS complaints related to mobile premium services”.

[189] See ACMA ‘Report spam’ http://www.acma.gov.au/Citizen/Stay-protected/My-online-world/Spamreporting-spam-i-acma (date of use: 20 January 2016).

Act does not cover certain instances provided on that site.[190] Through these services, consumer education and awareness has been served.

7.3.1.1 Recipients

The ACMA has developed educational strategies aimed, in the first instance at spam prevention, but which include how citizens needed to deal with spam when they receive it. A simple strategy included encouraging the public to deal with spam scams by either "ignor[ing] it", "report[ing] it", or "delet[ing] it".[191] ACMA also encourages the use of filtering software and network-level filtering by ISPs, and lastly it promotes its reporting facilities that allow users to forward SMS or e-mails directly in the format they are received.[192] Consumers (particularly young people who are increasingly exposed to targeted SMS marketing messages, are reluctant or indifferent when it comes to reporting such) are also encouraged to send messages as soon as they receive them so that the information can assist the ACMA in its investigations into breaches of the Spam Act.[193]

7.3.1.2 Businesses

Before the ACA and National Office for the Information Economy[194] were established, businesses carried out extensive awareness campaigns, including seminars and media interviews throughout Australia.[195] They also distributed official government guides for businesses, and provided information through the ACA web site.[196]

[190] Ibid. These instances included the following: "refunds and scams (in which a relevant forum is provided for those particular queries); voice telemarketing (consumers in this instance are urged to visit the do-not-call registry for complaints); the content of spam (consumers are advised to report such to ACMA's content "Clarification Section" if the content is deemed offensive); faxes (same as voice telemarketing); and mobile premium service (information is available from the ACMA web site)".

[191] Ibid.

[192] See ACMA 'Spam education and awareness' supra n 187. The direct forwarding options have become the preferred method of advising the ACMA of spam messages received by a substantial margin which more than 99% of messages received are directly forwarded.

[193] Ibid.

[194] Hereafter 'NOIE'.

[195] See ACMA 'Submission to Spam Act Review' supra n 1 23.

[196] Ibid.

On-going business education is undertaken principally through the ACMA web site, hotline, brochures, and the complaints system.[197] In order to identify companies that might not be aware of the Spam Act, the formal complaints system is used.[198] Usually the complaints are issued to companies which do not follow the standard requirements of the Spam Act as outlined above.[199] Depending on the severity of the problem, the first step is educational and informative contact with the company to ensure it is aware of its obligations and has appropriate processes in place to comply with them.[200]

In 2010 the ACMA delivered some initiatives as part of its cyber-safety program.[201] The Australian Direct Marketing Association (ADMA) also raises awareness in the marketing arena and offers education and certificates.[202]

7.3.1.3 Public awareness

The main portal for public awareness on how to prevent and report spam is the ACMA web site: www.acma.gov.au.[203] In 2006 the spam section of the web site received 400 000 hits. The public is also informed of enforcement, technical initiatives, and other developments, and business about the activities and the Spam Act, through regular media releases.[204] In addition, the ACMA has made available the use of podcasts on spam and e-security for small businesses, and is developing a consumer-focused podcast for a younger audience who are not consumers of

[197] Ibid.

[198] Ibid.

[199] Ibid.

[200] Ibid.

[201] The initiatives included: "a new cyber-smart parent resource (a research into the information needs of parents, including areas where most parents are concerned about the delivery channels that works best for them); an interactive e-learning platform to give teachers and schools more flexibility in accessing ACMA's very resourceful outreach program; pre-service teacher training program to be rolled out to universities across Australia; a new DVD for teenagers dealing with online privacy was introduced in 2011; also cyber-safety resources were made available in multiple languages to meet the information needs of non-English speaking Australians". See ACMA 'Joint Select Committee on Cyber-safety Submission No 80' (July 2010) 2 and 5 http://www.aphref.aph.gov.au-house-committee-jscc-subs-sub_80%20(3).pdf (date of use: 20 January 2016).

[202] ADMA is a leading industry body for Australian data driven marketing and the advertising industry. See ADMA 'Members Hub' https://www.adma.com.au/members-hub/overview/ (date of use: 20 January 2016).

[203] See ACMA 'Submission to Spam Act Review' supra n 1 23.

[204] Ibid.

traditional media.[205] The ACMA noted that despite the fact that ISPs are offering filters to consumers, consumers do not avail themselves of this help. The ACMAs response has always been to inform all members of the public who complain about the volume of unsolicited e-mails they receive, of the existence of these podcasts and to encourage their use.[206]

In addition to podcasts education is also conducted through a number of mediums including: giving interviews in all mediums, like TV, radio, print, and online.[207] Feedback indicates that this has been very successful in raising awareness of the Spam Act and other initiatives that the ACMA and the Australian government are undertaking to deal with spam.[208]

7.3.2 Industry measures

Industry has been noted as being in the frontline in combating spam, and is recognised as an essential element in government's anti-spam strategy. Responsible e-marketing business found that marketing channels were being flooded by the activities of spammers, and in the worst case scenarios, these activities by malicious spammers were harming public trust and confidence in e-commerce.[209]

The ACMA issued regulatory guidelines to assist industry and the community by offering practical guidance and explaining the principles underlying the ACMA's approach to spam activities.[210] The ACMA also adopted what is called a "graduated, strategic, risk-based approach" to combating spam which seeks to educate industry on its compliance obligations in an informal and constructive manner.[211] It also encourages a compliance culture among businesses and individuals engaged in e-

[205] Ibid.
[206] Ibid.
[207] Id 24.
[208] Ibid.
[209] See ACMA 'Submission to Spam Act Review' supra n 1 19.
[210] See ACMA 'Regulatory guides and guidelines' http://www.acma.gov.au/theACMA/About/The-ACMA-story/Regulating/regulatory-guides-guidelines-limitations-on-control-acma (date of use: 20 January 2016).
[211] See Australian National Audit Office 'Regulation of unsolicited communications' https://www.anao.gov.au/work/performance-audit/regulation-unsolicited-communications (date of use: 23 March 2017).

marketing and adherence to regulatory obligations[212] and e-marketing practices that are respectful of community standards, responsive to community complaints, and aim for best practice. The ACMA noted that the following stakeholders incur costs in dealing with spam, both in managing their infrastructure and in protecting their customers: ISPs; E-mail Service Providers (ESPs); and mobile phone companies.[213] These stakeholders also find themselves overwhelmed by complaints about spam being routed via customer machines on their networks.[214]

The development of industry codes of practice provide a vehicle for industry collaboration on the problem of spam and play an important role in supporting and ensuring the effectiveness of the Spam Act.[215] This is because codes and rules contained within the codes are relevant to industry's current practices and ways of doing business, and are most likely to be adhered to by industry which developed and endorsed them.[216] The efficacy of industry codes can be achieved through active promotion by government and key industry players and associations which will ensure that the relevant sectors of the industry are aware of the codes, and are also encouraged to sign-up to them.[217]

7.3.2.1 E-marketing code for spam: A code for ISPs

(a) Background to the Spam Code

The e-marketing code[218] was registered on 16 March 2006 to provide an outline of how the Spam Act applies to current e-marketing practices, and also to promote best practice use of CEMs in compliance with the Spam Act.[219] The Code was developed by the following stakeholders: the Internet Industry Association (IIA) in conjunction with the Internet Associations from Western and South Australia; consumer groups; message service providers; government regulatory agencies; and corporate

[212] Ibid.
[213] Ibid.
[214] Ibid.
[215] Ibid.
[216] Ibid.
[217] Ibid.
[218] Hereafter 'the Code'.
[219] See ACMA 'Spam code of practice' http://www.acma.gov.au/theACMA/Library/Industry-library/Marketers/spam-code-of-practice (date of use: 20 January 2016).

business.[220] The Code applied automatically to all persons, including individuals and organisations, undertaking an e-marketing activity (eg, ISPs and global ESPs offering services in Australia).[221] According to ACMA, the Code was developed to establish comprehensive industry rules and guidelines for the sending of CEMs with an Australian link in compliance with the Spam Act.[222] The Code's rules and guidelines provided specific and practical guidance in relation to the sending of CEMs in the context of the current e-marketing practices.[223] It also provided a framework by which industry could handle complaints about spam and monitor industry compliance with its provisions.[224]

Under the Code, e-marketing companies could subscribe to the Code and nominate a recognised industry body of which they were a member, to consider escalated complaints as to their compliance with the Code.[225] A signatory to the Code indicated its willingness and commitment to comply with the Code rules.[226] The Code's administrative body was made up of representatives from e-marketing industry associations, message service providers, and corporate business and was responsible for the on-going code administration.[227]

[220] See ACMA http://www.acma.gov.au/theACMA/Library/Industry-library/Marketers/spam-code-of-practice; also ACMA 'Australian eMarketing code of practice' supra n 13 4-6.

[221] See Lohman T 'ACMA to force anti-spam on ISPs' http://www.itnews.com.au/News/36262,acma-to-force-anti-spam-on-isps.aspx (date of use: 15 January 2016); and ibid ACMA 'Australian eMarketing code of practice'. An "e-marketing activity" is defined as and covers the following activities undertaken by an individual or organization: "to market, promote or advertise its own goods and services where sending or causing to send commercial electronic communications is the sole or principal means of marketing, promoting or advertising its own goods and services; that by contract (or other arrangement with) a person markets, advertises or promotes the goods or services (including land and interests in land and business and investment opportunities) of that person by sending CEMs or causing them to be sent; that by contract (or other arrangement with) a person markets, advertises or promotes that a person as a supplier, prospective supplier, provider or prospective provider of goods or services (including land and interests in land and business and investment opportunities) by sending CEM or causing them to be sent".

[222] Id ACMA 'Australian eMarketing code of practice' 3.

[223] Ibid.

[224] Id 3.

[225] See Australian eMarketing code signatory 'Application for signatory status under the Australian eMarketing Code of Practice' http://acma.gov.au/~/media/Unsolicited%20Communications%20Compliance/Form/pdf/Australian%20EMarketing%20Code%20of%20Practice%20Application%20for%20Signatory%20Status.pdf (date of use: 20 January 2016). Recognised industry bodies may apply to the ACMA for accreditation as a recognised industry body which, once appointed, will authorise that particular industry body to investigate and resolve complaints on behalf of its members that are signatories to the code; also ACMA 'Australian eMarketing code of practice' supra n 13 3.

[226] Ibid ACMA 'Australian eMarketing code of practice'.

[227] Ibid.

(b) Aims of the Code

The Code aimed to reduce the volume of UCEMs received by consumers and provided an e-mail service that offered spam filtering options to subscribers.[228] It also provided advice to subscribers on how to deal with and report spam, and also ensured that "acceptable use policies" prohibited the use of their networks for spamming and informed their subscribers accordingly.[229] It provided for compliance with requests from law enforcement and regulatory agencies investigating spam activities.[230] The Code allowed for an industry-based complaint-handling process with escalated complaints referred to nominated recognised bodies.[231] The Code also set out "safety net" provisions whereby complaints could be referred to the ACMA.[232]

In launching the Code Australia, as the first country to adopt a legislative code of practice for ESPs, was lauded as leading the way in the fight against spam.[233] The Code required ISPs and ESPs to inform end users of ways to combat spam and to have a process for handling complaints from subscribers in place.[234]

(c) De-registration of the code

In September 2014 a proposition was made in favour of de-registration of the Code.[235] A preliminary assessment suggested that due to technological developments and the evolution of the Internet industry (since the registration of the

[228] Id 15-19.
[229] Ibid.
[230] Ibid.
[231] Ibid.
[232] Ibid. In the first instance "any complaint about a breach of the code will be handled by e-marketing company to which the complaint relates. If the complaint is not handled to the satisfaction of the complainant, it will be referred to the recognised industry body nominated by the e-marketing company. However, if the complaint relates to an e-marketing company that is not a signatory to a code, or if it is a signatory to the code but has not nominated a recognised industry body, the ACMA will deal with the complaint. The complainant may request that his or her complaint be referred to the ACMA for consideration at any stage in the complaints handling process. The ACMA monitors the e-marketing industry's performance against the code rules and may require a company whose compliance appears to be inadequate to address any process problems or difficulties".
[233] Ibid.
[234] Ibid.
[235] See ACMA 'Proposed de-registration of spam code' http://www.acma.gov.au/theACMA/Consultations/Current/proposed-deregistration-of-spam-code (date of use: 20 January 2016).

code), certain obligations in the Code could be considered to no longer constitute standard industry practice and to have become irrelevant or outdated.[236] Accordingly, the Code was deregistered in October 2014.[237]

7.3.3 Technological initiatives and solutions

In 2006 the ACMA mandated ISPs and ESPs to provide spam-filtering options to their subscribers, even though three-quarters of all ISPs had already volunteered to offer spam-filtering products.[238] This included "SpamMatters" which assisted the ACMA to track down spammers by providing a simple one click method for the public to report malicious messages.[239] As noted above, SpamMatters is a customer friendly spam-reporting button enabling users to report and delete spam e-mails simultaneously by a single click.[240] Instead of using a delete key to remove the spam, users can select the SpamMatters button and simultaneously delete and report the spam e-mail to the ACMA.[241] The ISPs technical initiatives to prevent spam by introducing software that can assist users to stop spam was also introduced. To that end the ACMA as its first mandate, used forensic technology to collect and examine suspect e-mails to obtain evidence that could be used in a court action against spammers.[242]

In 2005 the Australian Internet Security Initiative[243] was launched as an initiative to help reduce malicious software (malware) infections and service vulnerabilities

[236] Ibid.

[237] Ibid.

[238] Ibid.

[239] See SPAMFighter 'ACMA Unleashes SpamMATTERS: the new anti-spam button' http://www.spamfighter.com/News-5995-ACMA-Unleashes-SpamMATTERS-the-New-Anti-Spam-Button.htm (date of use: 20 January 2016).

[240] According to ACMA 10% of spam e-mails sent were phishing spam that attempted to steal users' banking details and other vital personal information. This tool was set to provide more forensic evidence during spam fighting as the program was expected significantly to increase the amount of information collected by ACMA about spam creators. Ibid.

[241] See Internet Marketing Newswatch 'ACMA launches SpamMatters' http://www.Imnewswatch.com/2006/05/30/acma-launches-spammatters (date of use: 20 January 2016).

[242] See ZDNet 'Aust spam enforces turn to forensics for "dobbing" campaign' http://www.zdnet.com/article/aust-spam-enforcers-turn-to-forensics-for-dobbing-campaign/ (date of use: 20 January 2016). As noted above, in 2010 the ACMA launched its new reporting tool 'Spam SMS' which provides Australians with a quick and easy way of reporting spam by forwarding messages received to a specific number. See ACMA 'Spam SMS boosts the ACMA's fight against spam' http://www.acma.gov.au/theACMA/acma-media-release-692010-9-june-spam-sms-boosts-the-acmas-fight-against-spam (date of use: 20 January 2016).

[243] Hereafter 'AISI'.

occurring on the Australian Internet Protocol (IP) address ranges.[244] This started with six ISPs, and by the end of 2015 membership had risen to 146 which included 126 ISPs and eighteen educational institutions.[245] The ISPs participating in the AISI are estimated to cover more than 95 per cent of Australian residential Internet users.[246] These ISPs assist by raising security levels on Australian IP address ranges, which reduces costs for all ISPs and users.[247]

Through the AISI, daily e-mail reports are provided to ISPs which identify IP addresses on their networks which are perceived as being malware infected or potentially vulnerable to malicious exploitation.[248] The ISPs are encouraged to use the AISI data to identify and inform affected customers of their malware infection or service vulnerability.[249]

While two per cent of the spam in Australia came from within its borders in 2006, the remainder was from outside, hence the need to collaborate with other jurisdictions.[250] This is important, because the coming into operation of the Spam Act had the effect that spammers moved their activities outside of Australia's borders where connectivity is inexpensive but easy to exploit for spamming activities.[251]

7.3.4 International cooperation

As noted in the previous chapters (particularly Chapters 4 and 6) international cooperation is extremely important if one is to fight spam effectively, and the ACMA is at the forefront of international efforts to fight spam and improve e-security.[252]

[244] See ACMA 'Australian Internet Security Initiative (AISI)' http://acma.gov.au/Industry/Internet/e-Security/Australian-Intenet-Security-Initiative/australian-internet-security-initiative (date of use: 20 January 2016). This initiation also noted that malware infections are set to enable cyber criminals to steal personal and sensitive information from infected computers (also referred to as "botnets") and control them remotely for illegal or harmful purposes without the knowledge of the device user. Also see Australian Government 'More malware, adware, spyware, spam and spim' http://aic.gov.au/media_library/publications/htcb/htcb011.pdf (date of use: 20 January 2016).

[245] Ibid.

[246] Ibid.

[247] Ibid.

[248] Ibid.

[249] Ibid.

[250] Australian National Audit Office 'Regulation of unsolicited communications' supra n 211.

[251] ACMA 'Australian Internet Security Initiative (AISI)' supra n 244.

[252] See Australian National Audit Office 'Regulation of unsolicited communications' supra n 211.

Australia has also been recognised by organisations and telecommunication authorities for its work in the international spam community.[253] According to the ACMA, Australia has been consistent in world rankings by dropping spam from a list of relaying countries. In 2004 Australia was ranked tenth in the world, meaning that it was among the top ten countries in the world from which most of the spam e-mails were originating. In 2010 this "ranking" dropped to 25th on the list; and in 2013 it was ranked at 44th (meaning the least senders of spam per country) in the world.[254] It is noted that this decrease is partly due to the fact that Australia is a signatory to a number of multilateral and bilateral agreements with other countries some of which are highlighted below.[255]

7.3.4.1 Australia and Korea

In 2003 the Internet and Security Agency of Korea, the ACMA, and the NOIE of Australia, entered into MoU addressing cooperation in regulating spam.[256] The purpose of this MoU was to encourage cooperation between the signatories in minimising spam originating in and being sent to end-users in each country.[257] Cooperation between the signatories was in the form of exchanging information on spam and the establishment of appropriate channels for this exchange.[258] It further included the exchange of delegations, visits, and the encouragement of liaison between industry and government organisations to promote areas of interest and cooperation.[259] The MoU was to remain effective for five-year years unless terminated by the signatories giving six months' notice.[260]

[253] Ibid.

[254] Ibid.

[255] See ZDNet 'Anti-spam assault spans Asia-Pacific' http://www.zdnet.com/article/anti-spam-assualt-spans-asia-pacific (date of use: 15 January 2016).

[256] See *The Memorandum of Understanding Between the Korean Information Security Agency and the Australian Communications Authority and the National Office for the Information Economy of Australia Concerning Cooperation in the Regulation of Spam* 1-3 http://www.itu.int/osg/spu/spam/contributions/Attachments%20Memorandum%20of%20Understanding%20Between%20KISA%20ACA%20and%20and%20NOIE.pdf (date of use: 20 January 2016). Hereafter 'MoU Australia and Korea'.

[257] Id para 2. See also Relf supra n 2 118.

[258] MoU Australia and Korea supra n 256 para 2.

[259] Id 2.

[260] Id paras 12-14.

7.3.4.2 Seoul and Melbourne

This MoU was entered into between Seoul and Melbourne in an effort to minimise spam[261] originating in either country or region, passing through either country or region, and being sent to end-users in either country or region.[262] The MoU recognised that bilateral and multilateral cooperation could complement areas of mutual interest in reducing the spam problem, and identified areas of common interest for cooperation. This included, but was not limited to, the encouragement of the exchange of information, which covered policies and strategies for establishing and enforcing anti-spam regulatory frameworks;[263] technical and educational solutions to the spam problem;[264] and strategies for the effective use of regulation policies in support of enforcement.[265] The exchange of intelligence relating to other countries or regions gathered as a result of enforcement and industry collaboration, and also anti-spam measures and emerging issues were encouraged.[266]

Other areas of concern in the MoU included: the exchange of delegations and visits as appropriate; encouragement of liaison between industry and government organisations to promote areas of interest and cooperation; and other forms of cooperation arranged bilaterally or multilaterally by signatories.[267] The MoU was approved on 27 April 2005 and in the same year was expanded to include thirteen organisations from ten economies in the Asia-Pacific region in order to better achieve global solutions to a global problem.[268] The duration of the MoU was initially

[261] *Seoul-Melbourne Multilateral Memorandum of Understanding on Cooperation in Countering Spam* 1-7 http://www.sm-mou.org/smmou/about_mou.php (date of use: 20 January 2016). Hereafter 'MoU Seoul-Melbourne'.

[262] Id para 2.

[263] Id 1-2.

[264] Ibid.

[265] Ibid.

[266] Ibid.

[267] Id 2. In the case of changes in the anti-spam legislation of a signatory and signing of other agreements, the signatories will use their best efforts to consult with the other signatories promptly, either directly, indirectly, or through the Secretary of Signatories, as to whether such modifications may have implications for the operation of the MoU, and whether the MoU should be amended. The same will apply where signatories are considering becoming a party to another agreement that may have implications for the operation of this MoU.

[268] Ibid. The goals of the revised MoU are the development of: (a) policies and strategies for establishing and enforcing anti-spam regulatory frameworks; (b) technical and educational solutions to the spam problem; (c) the effective use of policies in support of enforcement; and (d) industry collaboration.

three years from the date of signature, but its validity was extended to end in May 2013.

7.3.4.3 Australia and the Kingdom of Thailand

Other partnership agreements include a joint statement issued in conjunction with the Ministry of Information and Communication Technology of the Kingdom of Thailand in 2004.[269] Under this joint statement the relevant institutions in Australia and Thailand, agreed to cooperate in matters of mutual interest through the exchange of ideas, information, personnel, skills and experiences, and collaborative activities that will be of benefit to both sides.[270]

Areas of participation include, among others,[271] exchanging information about anti-spam policies and strategies, security issues and other identified areas of interest of both countries.[272] This joint statement entered into force on 5 July 2004, and is to remain in force subject to availability of funds and resources.[273]

7.3.4.4 Australia, United Kingdom and United States

In 2004 an MoU to regulate spam was entered into by the United Kingdom's Information Commissioner, the United States' Federal Trade Commission, Australia's Competition and Consumer Commission, and the ACA.[274] The purpose of

[269] See *Joint Statement between the Department of Communications Information Technology and the Arts (Australia) and the Ministry of Information and Communication Technology of the Kingdom of Thailand Concerning Cooperation in the Fields of Communications and Information Technology* 1-2 http://www.acma.gov.za.au (date of use: 20 January 2016). Hereafter 'Australia and Thailand Joint statement'.

[270] Id 1.

[271] Other areas include: exchanging information to telecommunications policy and regulatory matters and on the application of information technology; exchanging knowledge about participation in the activities of specialised international organisations; cooperating on the implementation of the other stakeholders; and Telecommunications and Information Working Group Mutual Recognition Arrangement. See APEC 'What is Asia-Pacific Economic Cooperation?' http://www.apec.org/About-Us/About-APEC.aspx (date of use: 20 January 2016).

[272] Id 1-2.

[273] Id 2.

[274] See *The Memorandum of Understanding on continual enforcement assistance in commercial email matters among the following agencies of the United States; the United Kingdom and Australia: The United States Federal Trade Commission; the United Kingdom's Office of Fair Trading; the United Kingdom's Information Commissioner; Her Majesty's secretary of State for Trade and Industry in the United Kingdom; the Australian Competition and Consumer*

this MoU is "to share evidence by recognising the three countries common interests in facilitating effective enforcement to combat spam violations; and to avoid unnecessary duplication, and facilitating sequential, simultaneous or coordinated investigations of spam violations, or suspected spam violations; and to exchange and provide appropriate information".[275]

In furthering their common interests, the participants intend to use best efforts to exchange and provide appropriate information in relation to consumer and business education.[276] It further includes investigations and research in relevant areas, including practices such as address harvesting, dictionary attacks, and compliance education programs.[277] Other objectives include the provision or obtaining of evidence that could assist in determining whether a person has committed or is about to send spam in violation of the provision, or in facilitating the administration or enforcement of measures aimed at spam.[278] Parties also need to inform one another of spam violations occurring in their territories,[279] and to discuss evidence in their possession by using best efforts to cooperate in the detection and investigation of spam violations.[280] This MoU is to be reviewed on an annual basis regarding cooperation, coordination, and enforcement assistance undertaken among the participants.[281]

7.3.4.5 Australia and Taipei

In 2007 the Australian Commerce and Industry Office in Taipei and the Taipei Economic and Cultural Office entered into an MoU.[282] The MoU acknowledged that

Commission; and the Australian Communications Authority 1-11 http://www.ftc.gov/sites/default/files/attachments/international-antitrust-and-consumer-protection-cooperation-agreements/040630spammoutext.pdf (date of use: 20 January 2016). Hereafter 'MoU Australia, UK and USA'*.*

[275] Ibid.

[276] Id para II B.

[277] Id. These include: self-regulatory and technical enforcement solutions; amendments to relevant legislation; and staffing and resource issues, including the possibility of staff exchanges and visits.

[278] Id para II C.

[279] Id para II D.

[280] Id para II E.

[281] Id para X.

[282] See *Memorandum of Understanding between Australia Commerce and Industry Office, and the Taipei Economic and Cultural Office in Australia Concerning Cooperation in the Cooperation in the Regulation of Spam* (signed October 2007) 1-4 http://www.acma.gov.au/~/media/

the protection of the information economy is a major factor for social, economic, and environmental development, and for the realisation of productivity and improvement of service delivery in all sectors of the economy.[283] The MoU noted that since spam could impair the infrastructure and viability of the information economy, mutual cooperation could minimise the volume of spam flowing between economies and assist in combating the spam problem.[284]

The purpose of this MoU was to encourage cooperation between the signatories in minimising spam originating in and being sent to end users in their respective economies.[285] Signatories where also encouraged to cooperate more closely in the exchange of information relating to spam in accordance with the relevant laws and regulations in each economy and on the basis of equality, reciprocity and mutual benefit.[286] The MoU also encouraged the exchange of information about policies and strategies for establishing and enforcing anti-spam regulatory frameworks.[287] Parties further agreed to discuss the effective use of regulation policies,[288] and to exchange intelligence relating to the other countries gathered as a result of enforcement investigations and industry collaboration.[289]

In order to coordinate cooperative activities each signatory was mandated to appoint a representative responsible for determining the particular directions of cooperation and for ensuring the effectiveness of all cooperation and exchange activities.[290] Signatories also agreed to consult with one another through specified channels to

Unsolicited%20Communications%20Compliance/Information/pdf/Spam%20International%20Cooperation%20Memorandum%20of%20Understanding%20Between%20Australia%20and%20%Taiwan.Pdf (date of use: 20 January 2016). Hereafter 'MoU Australia and Taipei'.

[283] Id 1.

[284] Ibid.

[285] Ibid.

[286] Ibid.

[287] Id paras 3 and 4. The cooperation between the signatories in the field of regulating spam may take the following form: exchange of information on spam, and establishment of channels for exchange of information as appropriate; exchange of delegations and visits as appropriate; encouragement of liaison between industry and nominated organisations to promote areas of interest and cooperation; and other forms of cooperation arranged by the signatories.

[288] Ibid.

[289] Ibid.

[290] Ibid.

define activities and other related matters.[291] This MoU was to remain effective for a five-year period unless terminated by the signatories on six months' notice.[292]

7.3.4.6 Australia and New Zealand

In 2009 the ACMA joined forces with New Zealand's Department of Internal Affairs to establish channels of communication that would allow both agencies to move quickly in response to the challenges and demands of the ever-changing spam environment.[293] The purpose of this MoU was to facilitate cooperation, assistance, and the exchange of information, including confidential information relevant to the regulatory functions of each Agency.[294] The MoU also made provision for information, documents, and assistance to be provided regarding unsolicited information.[295] It also provided for requests for assistance on compliance and enforcement, procedures for requests for information or documents, and also for permission to use the information.[296] This MoU was to remain effective for three years unless it was terminated by the signatories giving a six months' notice.[297]

7.4 Conclusion

In this chapter the five-fold regulation strategy for combating spam in Australia was outlined. Apart for its comprehensive anti-spam legislation, Australia has also equipped its consumers and citizens by educating and promoting awareness of the problem. Even where the consumers appear complacent, the ACMA is at the forefront in ensuring that consumers are not only aware of the dangers facing them when it comes to spam, but has also made tools available to assist them in combating spam. This education and awareness is available to all, especially the young and the elderly through all mediums of communication.

[291] Id para 5.
[292] Id para 10.
[293] See *Memorandum of Understanding between the Australian Communications and Media Authority (ACMA) and the New Zealand Department of Internal Affairs (DIA)* 1-10 http://www.acma.gov.au/~/media/Unsolicited%20Communications%20Compliance/Information/pdf/Spam%20International%20Cooperation%20Memorandum%20Understanding%20Between%20Australia%20and%20New%20Zealand.PDF (date of use: 20 January 2016). Hereafter 'MoU Australia and New Zealand'.
[294] Id para 3.2.
[295] Id paras 5-11.
[296] Ibid.
[297] Id para 17.

The marketing industry, too, is playing its part in combating spam with industry players holding each other accountable and educating marketers on how to comply with the provisions of the Spam Act. While spam is an on-going problem, Australia is a good example of a jurisdiction which is aware of the escalating problem and is actively involved in implementing measures to combat spam and ensure adequate protection. Australia is also active in the global arena playing its part by forming partnerships with other countries and or organisations in an effort to combating spam. The implementation of a multi-faceted solution has also proved to be effective in minimising spam within Australia's boundaries and also limiting the spam leaving its boundaries.

This is a far cry from the South African regime for combating spam as is shown in the following chapter where the South African position is considered.

CHAPTER 8

A COMPARATIVE STUDY OF ANTI-SPAM LAWS: A SOUTH AFRICAN PERSPECTIVE[1]

8.1 Introduction

In the last two chapters a discussion on anti-spam laws, in particular those of the USA and Australia was highlighted. This chapter continues in the same vein, but now focus is on South Africa. South Africa does not have a single, fully-fledged anti-spam Act. Rather, spam is regulated in a number of legislation addressing various issues.[2] These include the first anti-spam provisions in the Electronic Communications and Transactions Act,[3] followed by a number of consumer-oriented laws which will be addressed below.[4] Three Bills have also been published which contain spam-related matters: a proposed Amendment[5] to the ECT Act; and two Bills on Cybercrime and Cybersecurity.[6]

In this chapter focus is on these legislative provisions through an examination of: their background; the purpose of the specific piece of legislation; a consideration of their anti-spam and direct-marketing provisions; commentary on those provisions, including the benefits of a particular anti-spam provision (if any); criticisms levelled at particular provisions (if any); and, where applicable, solutions will be highlighted. An examination of case law is also made to establish how the court(s) have interpreted the relevant provisions. Further published Bills will be highlighted. In conclusion, a

[1] Some sections of this chapter formed part of the conference proceedings: Tladi 'SPAM: An Overview' 266-78. The chapter is also a continuation of the following works: Pistorius & Tladi (2014) *SA Merc LJ* 688-705; and Tladi 2008 *SALJ* 178-92.

[2] These anti-spam provisions are contained in legislation covering electronic transactions and communications, consumer protection, the protection of personal information, or data protection, to name but a few.

[3] The Electronic Communications and Transactions Act 25 of 2002 (hereafter the 'ECT Act').

[4] These laws include: National Consumer Credit Act 34 of 2005; the Consumer Protection Act 68 of 2008; and the Protection of Personal Information Act 4 of 2013.

[5] See the Electronic Communications and Transactions Amendment Bill *Government Gazette GG* No. 35821 Notice 888 (26 October 2012) http://www.ellipsis.co.za/wp-content/uploads/2012/10/Electronic-Communications-and-Transactions-Amendment-Bill-2012-for-public-comments-20121026-GGN-35821-00888.pdf (date of use: 30 November 2015).

[6] See the Cybercrimes and Cybersecurity: Bill (Draft for Public Comment) *Government Gazette GG* No. 39161 Notice 878 (30 November 2015) http://www.justice.gov.za/legislation/notices/2015/20150902-gg39161_gen878-cyberbill.pdf (date of use: 20 January 2016); and Cybercrimes and Cybersecurity Bill *Government Gazette GG* No. 40487 (9 December 2016) http://ellipsis.co.za/wp-content/uploads/2017/02/b-6-2017-cybercrimes.pdf (date of use: 4 March 2017).

contextualisation of the various anti-spam provisions to establish whether harmonisation and alignment of these laws is necessary in formulating a model law for South Africa will be highlighted. The ECT Act will start the discussion, followed by other anti-spam and direct-marketing provisions.

8.2 The ECT Act 25 of 2002

8.2.1 Background to the ECT Act

The ECT Act resulted from the Green paper on electronic commerce (e-commerce) prepared by the Department of Communications in 2000.[7] In its executive summary, the Green Paper contained four categories outlining key issues or areas of concern that needed serious consideration in e-commerce policy formulation.[8] One of those categories was the need for confidence in the security and privacy of transactions performed electronically.[9] In addressing the issue of consumer confidence, the Green Paper highlighted the dangers from which consumers needed to be protected, including unsolicited goods and communications (spam) and dangers related to the invasion of privacy,[10] to name but a few.[11] These dangers reveal the need to protect consumers at every stage in their online transaction or communication. The Green paper led to the promulgation of the ECT Act in 2002.[12]

[7] The Department of Communications 'The Green Paper on e-commerce: Making it your business' (2000) hereafter 'the Green Paper'. The Green Paper was a consultative document designed to raise questions on issues that needed to be addressed by government policy formulation. It provided a platform from which topical issues around e-commerce could be translated into government policy. The Green Paper built on the discussion paper published in October 2000; followed by the White Paper in the second quarter of 2001; and specific legislation in the third and fourth quarters of 2001 (see the Green Paper 10-11) and Groenewald 'Towards an electronic commerce policy for South Africa' 106-112 for a discussion on electronic commerce policy for South Africa.

[8] See the Green Paper 9.

[9] Id 6. Other categories included the need to: enhance the information infrastructure for electronic commerce; establish rules that will govern electronic commerce; and bring the opportunities of e-commerce to the entire population. According to the Green Paper, "these categories give a general background to specific issues; discuss challenges and problems; and also paint an international as well as a national picture while posing policy questions relating to the issue".

[10] These two dangers later formed the provisions in the ECT Act contained in ss 45, 50 and 51 respectively. These provisions are outlined below.

[11] See the Green Paper supra n 7 47. Other dangers include: dangers resulting from the ease and convenience of buying online; insufficient information about goods and services; the risk of being deprived of protection through unfamiliar, inadequate or conflicting laws of a foreign country being applicable to the contract; the easy access to a web site; and cyberfraud.

[12] The ECT Act was signed into law on 31 July 2002.

8.2.2 The purpose of the ECT Act

The ECT Act applies to any electronic transaction or data message in the Republic.[13] The objectives of the ECT Act are listed in section 2(1) as among others:[14]

> to enable and facilitate electronic communications and transactions in the public interest, and, to that end to, among others: remove and prevent barriers to electronic communications and transaction in the Republic; …promote legal certainty and confidence in respect of electronic communications and transactions; …ensure that electronic transactions in the Republic conform to the highest international standards; …develop a safe, secure, and effective environment for the consumer, business, and the government to conduct and use electronic transactions; …and promote the development of electronic transaction services which are responsive to the needs of users and consumers.

The ECT Act contains fourteen chapters covering a variety of issues. Of importance to this study is Chapter 7 dealing with consumer protection issues.[15]

8.2.3 Consumer protection principles under the ECT Act

Chapter 7 applies only to electronic transactions.[16] Although there are a number of provisions in this chapter,[17] focus is mainly on the issue of unsolicited communications (spam) in section 45. Sections 50 and 51 which deal with data protection principles will also be considered. The consumer protection provisions

[13] See s 4(1) of the ECT Act.

[14] Ibid s 2(1)(d); (e); (h); (j); and (k). For a discussion of the facilitation of electronic transactions see: Coetzee (2004) 3 *Stell LR* 501-21; Meiring R 'Electronic transactions' 82-108; and Gereda 'The Electronic Communications and Transaction Act' 268-74.

[15] Most of the provisions in Chapter 7 fall outside of this study. However, the following works in which consumer protection under the ECT Act has been canvassed extensively by other commentators can be consulted: De Stadler *Consumer Law Unlocked* 136-40; Papadopoulos 'Online consumer protection' 64-79; Papadopoulos (2012) 75 *THRHR* 224-6; Neels (2010) 31/ 1 *Obiter* 123-5; Eiselen 'E-commerce' 198-210; Snail (2007) 15/2 *JBL* 54-60; Jacobs (2004) 16/4 *SA Merc LJ* 556-67; Buys 'Online consumer protection and spam' 139-60; and id Gereda 276-8.

[16] See s 42(1) of the ECT Act. This chapter does not apply to a regulatory authority established in terms of a law if that law prescribes consumer protection provisions in respect of electronic transactions (s 42(3) of the ECT Act). The exceptions to the application includes s 44 (covering the cooling off clause) which does not apply to electronic transactions for financial services, or the supply of foodstuffs, beverages or any other goods intended for everyday consumption (s 42(2) (a)-(j) of the ECT Act).

[17] The provisions in Chapter 7 include: the scope of application (s 42); information to be provided (s 43); performance (s 46); applicability of foreign law (s 47); s 48 (non-exclusions); and s 49 (complaints to Commission).

under the ECT Act raise duties on the side of the vendor and third parties.[18] They also create certain rights for the consumer.[19]

8.2.4 Data protection principles under the ECT Act

Chapter 8 deals with the protection of personal information[20] obtained by electronic means.[21] This chapter outlines eight specific principles to which a data controller[22] may subscribe. These principles cover the collection, collation, processing or disclosure of personal information on the data subject by the data controller.[23] However, subscription to these principles is voluntary.[24]

Roos notes that:[25]

> The major deficiency in these provisions is that they do not impose legally binding obligations on data controllers. This means that should the data controller choose not to subscribe to the data privacy principles, the data subject will have no redress other than delictual remedies. Furthermore, there is no external supervisory body or criminal sanctions to enforce the principles and also no mechanism allowing the individual to enforce their rights rapidly and effectively.

[18] See s 43(1) of the ECT Act. The vendor should provide the following information to consumers: Its full name; its physical address and telephone number; its web site address and e-mail address; and the terms of agreement, including any guarantees, that will apply to the transaction and how those terms may be accessed, stored, and reproduced electronically by consumers.

[19] These include: a consumer being entitled to cancel the transaction (without reason and without penalty) within seven days after the receipt of goods or services after the conclusion of the agreement (id s 43(3)); the right to be given an option to cancel his or her subscription to the mailing list of the third party, and also to be provided with the source from which that supplier received or obtained the consumer's personal information (id s 45(1)).

[20] Section 1 of the ECT Act defines the term "personal information" as "information about an identifiable individual, including but not limited to: information relating to race, gender, sex, language et cetera; information relating to the education or the medical, criminal, employment history of the individual; any identifiable number, symbol, or other particular assigned to the individual; the address, fingerprints; and the name of the individual where it appears with other personal information relating to the individual or where the disclosure of the name itself would reveal information about that person".

[21] Id s 50(1).

[22] Section 1 of the ECT Act defines the term "data controller" as "any person who electronically requests, collects, collates, processes or stores personal information from or in respect of a data subject".

[23] Id s 51. These include the written permission of the data subject for collection or processing of their personal information (s 51(1)) and disclosure by the data controller in writing to the data subject of the specific purpose for which that information is being requested (s 51(3)). See Roos 'Data privacy law' 426-427; Roos 'Data Protection' 361-4; also Papadopoulos & Snail 'Privacy and data protection' 299; and Goodburn & Ngoye 'Privacy and the Internet' 174-5 a discussion of these principles.

[24] See s 50(2) and 50(3) of the ECT Act.

[25] Roos 'Data privacy law' 427-428.

Note should be taken here that sections 50 and 51 will be revoked once the Protection of Personal Information Act provisions come into effect. Below the anti-spam provisions in section 45 of the ECT Act are discussed.

8.2.5 Commentary on section 45 of the ECT Act

8.2.5.1 Anti-spam provisions under the ECT Act

As stated above, the first anti-spam provisions[26] in South Africa are contained in section 45 of the ECT Act. The title of this section is "unsolicited goods, services or communications". Section 45 reads as follows:

> (1) Any person[27] who sends unsolicited commercial communications to consumers must provide the consumer:
> (a) With the option to cancel his or her subscription to the mailing list of that person; and
> (b) With the identifying particulars of the source from which that person obtained the consumer's personal information, on request of the consumer.
> (2) No agreement is concluded where a consumer has failed to respond to an unsolicited communication.
> (3) Any person who fails to comply with or contravenes subsection (1) is guilty of an offence and liable, on conviction, to penalties prescribed in section 89(1).
> (4) Any person who sends unsolicited commercial communications to a person who has advised the sender that such communications are unwelcome, is guilty of an offence and liable, on conviction, to the penalties prescribed in section 89(1).

8.2.5.2 Benefits of the anti-spam provisions under the ECT Act

The benefit of the anti-spam provisions in the ECT Act is that they fulfil the Act's purpose of facilitating electronic communications and transactions in the public interest. The section has to an extent been aligned to international best practices by joining a host of countries with anti-spam laws or anti-spam provisions.[28] Section 45

[26] For a discussion of spam in South Africa see the following works: Eiselen 'E-commerce' 207-210; Swales (2016) 28/1 *SA Merc LJ* 49-84; Maheeph *Electronic Spamming* 1-66; Hamann & Papadopoulos (2014) 47/1 *De Jure* 42-62; Pistorius & Tladi (2014) 26/3 *SA Merc LJ* 688-705; Tladi 'SPAM: An overview' 266-78; Papadopoulos supra n 15 223-40; Tladi (2008) 25/1 *SALJ* 178-92; Sibanda (2008) 1 *Journal of Information Law & Technology* 1-9; Ebersöhn (2004) 12/3 *JBL* 137-42; Geissler *Bulk Unsolicited Electronic Messages* 1-403; Buys supra n 15 160-6; Gereda (2003) *De Rebus* 51-2; Ebersöhn (2003) *De Rebus* 25-6; Haase J.W; Grimm & Versfeld *International Commercial Law* 123-70; and Chigona et al 'Perceptions on SPAM in a South African context' *Internet and Information Technology in Modern Organisations: Challenges and Answers* 283-291 http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.515.745&rep=rep1&type=pdf (date of use: 20 January 2016).

[27] Section 1 of the ECT Act defines the term person as including a public body.

[28] Id s 2(1)(h) and Chapter 4 above, in particular para 4.3.4.2 (a) which addresses the requirements for crafting a strong anti-spam law.

also addresses the barriers inherent in an online environment and promotes consumer confidence in electronic communications.[29] It also contributes to a safe, secure, and effective environment for both consumers and businesses.[30] However, these benefits are not without problems and over the years commentators have levelled criticisms of section 45.[31]

8.2.5.3 Criticisms levelled at section 45 of the ECT Act

(a) Spam regulated and not prohibited

Section 45 of the ECT Act has been referred to as a "low-key" approach to regulating spam[32] in that its provisions do not prohibit spam but merely regulate it by giving consumers[33] certain rights which they can enforce against the sender.[34] These rights include the provision of an option to cancel the recipients' subscription from the sender's mailing list.[35] This provision has been criticised as confirming the existence of a particular e-mail address which results in the consumer receiving yet more spam.[36] Problems arising from the opt-out mechanism as noted above, include the fact that most if not all spammers disguise their header information when sending spam e-mail – for example, by concealing their particulars or using a third party's domain name. This, in turn, makes it difficult for consumers to unsubscribe from the spammer's mailing list as he or she is difficult to trace. Section 45, unlike its USA and Australian counterparts, provides only that there be an opt-out mechanism. There is no prescribed procedure on how opt-out request(s) will be administered by the sender or the time frames within which the request must be processed.[37]

(b) Lack of a definition(s)

[29] As highlighted in the Green Paper supra n 7 75-81.

[30] See n 14 above on the purpose of the ECT Act.

[31] See generally Tladi supra n 26 186-8 for the criticism levelled against s 45.

[32] See Eiselen supra n 26 207.

[33] Section 1 of the ECT Act defines the term "consumer" as "a natural person who intends entering into an electronic transaction with a supplier as the end user of the goods or services offered by the supplier".

[34] See Buys supra n 15 165 and Sibanda supra n 26 4.

[35] See s 45(1) of the ECT Act.

[36] See Gereda supra n 26 52.

[37] See Tladi supra n 26 186-7. Also contrast with: paras 5.3.4.2 (d) (Chapter 5); para 6.3.2.2 (Chapter 6); and 7.2.3.2(c) (Chapter 7).

Spam, as indicated earlier, is generally defined as unsolicited bulk mail or unsolicited commercial mail.[38] From the title of section 45 it is clear that spam is described from a commercial view hence the terms: “unsolicited commercial communications”, and “unsolicited goods and services”. These terms align with those found in the USA and Australia above.[39] Although these terms are used to describe spam, the ECT Act nonetheless fails to define what exactly the terms mean – a lack which some have found problematic in that it excludes other, equally irksome, forms of spam.[40] This concern was highlighted in earlier chapters.

(c) Harvesting e-mails and the sale of lists

The ECT Act does not specifically cover the issue of the harvesting and sale of lists, neither does it address the use of software to gather e-mail addresses for sending spam e-mails.[41] However, others are of the view this may be covered by sections 50 and 51 of the ECT Act.[42] As noted, the problem with the data collection principles under the ECT Act, is that they are not only voluntary, but as some have noted, such data can be collected by other means – for example, the use of cookies, web crawlers, et cetera – not covered by the ECT Act.[43] As emerged from the discussion of the USA and Australia above, the practice of harvesting and selling lists and related practices are prohibited activities punishable by law.[44] If these issues were to be investigated, the burden would be shifted from the consumer to the spammer, and the spammer would be held accountable for these deceptive practices. The

[38] See in particular Chapter 6 above. Also see the following: Geissler supra n 26 28-32 where the author discusses the difference between UBE and UCE; Gereda supra n 26 51; Tladi supra n 26 179-80; and Hamann & Papadopoulos supra n 26 47-9.

[39] For a discussion of these terms see: Chapter 6 para 6.3.2.1 (USA); and Chapter 7 para 7.2.3.1 (Australia) above. See also: the AU Convention (5.3.2.2(c) (ii); the COMESA Model Law on e-commerce (5.3.3.3); and the SADC Model Law on e-commerce (5.3.4.2).

[40] See Buys supra 15 160-1, where it is noted that: “non-commercial e-mail such as newsletters, opinion surveys, religious messages, political content, hoaxes, et cetera, do not fall under that term, and also that the ECT Act does not provide clarity on whether a communication must be in electronic format in order to be classified as spam”. Despite the lack of definition, the following elements can be deduced from these terms: unsolicited; commercial; and even bulk. For a discussion of these elements see the following: Ibid; Gereda supra n 26 51; Geissler supra n 26 24-8; Tladi (2008) supra n 26 180; Sibanda supra n 26 4; and Papadopoulos supra n 15 233-4.

[41] See Tladi supra n 26 188. See in particular Chapter 3 para 3.2.3 and 3.2.4 above where this issue is dealt with.

[42] See Smith (2004) 16 *SA Merc LJ* 599-601.

[43] Id 600; and Ebersöhn (2004) supra n 26 741 ff.

[44] Contrast with the following: para 4.3.4.2 (Chapter 4); para. 6.3.2.3(c) (Chapter 6); and para 7.2.3.2 (d) (Chapter 7) where this issue is addressed.

practice of harvesting is responsible for the increase in spam in other mediums, especially on mobile phones.[45]

(d) Fraudulent headers and spoofing

If an opt-out mechanism is to be effective, senders of spam e-mails must make their particulars available to recipients of such e-mails. The practice of disguising headers, or spoofing,[46] is problematic in the sense that if an opt-out process lacks the mechanism to opt-out efficiently, recipients will not be able to unsubscribe from future unwanted mail. Consequently, the sender would not be in a position to receive and process opt-out requests and thus refrain from sending more spam.

Unlike the position in the USA and Australia where such practices are prohibited,[47] the ECT Act does not address the use of fraudulent headers or the use of third-party domains in order to send spam.[48] Some, however, argue that this issue could be covered under sections 86 and 87 of the ECT Act.[49]

(e) Enforcement issues

Enforcement in this case will take place within borders. Buys is of the opinion that "practical issues such as the gathering of evidence, and the fact that most spam messages have no indication of the sender's location, together with jurisdictional barriers result in major law enforcement problems".[50] While the ECT Act also fails to address the issue of trans-border spam and how the Act will apply should spam

[45] For a discussion of e-commerce and mobile commerce in South Africa, SMS marketing, and direct marketing and spam, see: Jobodwana (2009) 4 *Journal of Information Law & Technology* 287-98; Jansen van Ryssen (2004) 4 *Acta Commercii* 48-59; Papadopoulos supra n 15 63-4; Hamann & Papadopoulos supra n 26 44-5; and Chigona W et al supra n 26 283-291.

[46] For the discussion on spoofing see Ebersöhn (2003) supra n 26 25-6; Tladi supra n 26 182; and para 3.2.6 (Chapter 3); and para 4.3.4.2(c) (iii) (Chapter 4).

[47] Contrast with the following provisions: paras 6.2.2.4 and 6.3.2.3 (a) and (b) in Chapters 6; and para 7.2.3.2(b) in Chapter 7.

[48] See Buys supra n 15 165 and Tladi supra n 26 187.

[49] See Snail (2009) 4 *Journal of Information Law & Technology* 5-7; Sibanda supra n 26 5; Buys supra n 15 165; and Ebersöhn (2003) supra n 26 25. Section 86 deals with unauthorised access to, interception of, or interference with data; and s 87 covers computer-related extortion, fraud, and forgery. These provisions are located in Chapter XIII of the ECT Act which deals with cybercrime.

[50] See Buys supra n 15 164.

originating from beyond SA's borders,[51] the USA and Australia have clear measures in place to address this eventuality.[52]

(f) Penalties

Section 89 of the ECT Act provides for penalties resulting from non-adherence to the provisions of the ECT Act. A person convicted of an offence referred to in specific sections,[53] is liable to a fine of one million Rand or to imprisonment for a period not exceeding twelve months.[54] Interestingly, the above provision is housed in a chapter dealing with cybercrime, but, as noted above, section 45 does not criminalise spam but regulates it. Furthermore section 45 does not fall under the provisions in section 89.[55]

Other criticisms include that section 45 does not address the interests of ISPs who come under "attack" from spammers.[56] Gereda notes that this is evident from the fact that "while consumers can request to be removed from the spammer's mailing list(s), the ISP incurs losses from the very spam it receives and has to manage".[57] In light of these criticisms, solutions have been suggested for the improvement of section 45.

8.2.5.4 Solutions to improve section 45

(a) Institute an opt-in model and other solutions

In light of the criticism above, certain commentators have suggested that South Africa should enact a "model law on spam" which adopts an opt-in mechanism as its default in preference to the current opt-out mechanism.[58] As noted in Chapter 6, this

[51] Id 165 for instances where the courts will have jurisdiction over spam-related criminal acts.

[52] See the issue of international cooperation between the USA (para 6.5.4 Chapter 6); and Australia (para 7.3.4 Chapter 7). Also see: para 4.3.4.6 (ITU); and para 4.4.2.3 (OECD) in Chapter 4.

[53] These include: s 37(3); 40(2); 58(2); 80(5); 82(2) or 86(1), (2) or (3) of the ECT Act.

[54] See s 89(1) of the ECT Act.

[55] See Tladi (2008) supra n 26 187.

[56] See Gereda supra 26 52.

[57] Ibid. Gereda note that "this is because the ISP carries the e-mail addresses of thousands of consumers who in turn only receive at least one spam e-mail in terms of the ECT Act before they can request that their e-mail addresses be removed from the spammer's list". Also see Chapter 3 para 3.3.1 where the costs incurred by ISPs are outlined.

[58] See especially Haase, Grimm & Versfeld supra n 26 157 and Geissler supra n 26 387-403.

is the solution that commentators in the USA were calling for, either to replace the opt-out mechanism, or to supplement it.[59]

(b) A multi-layered solution

Tladi notes that "given the global nature of spam, global measures need to be put in place if this scourge is to be eliminated which would include a multi-layered approach involving legislation, technical solutions, and consumer education".[60] Buys points out that "consideration should be given to the application of three general measures to address spam adopted in other jurisdictions including: informal measures such as self-regulation; technical measures undertaken by individuals and organisations; and litigation and legislation".[61]

(c) Other suggestions

Ebersöhn suggests that as section 45 lags behind corresponding foreign legislation it should be amended to prohibit: harvesting and dictionary attacks; the use of false and misleading e-mail headers; and the inclusion of labels such as "ADV" in the subject lines.[62] He also notes that "those responsible for the ECT Act should be required to review the efficacy of section 45 on a regular basis,[63] an evaluation which might result in measures to combat spam being added or discontinued where they are found no longer to meet the needs of that jurisdiction".[64]

The solutions above align with anti-spam laws and provisions noted in the previous chapters – in particular on how to draft an anti-spam Act and also to combat spam at a global level.[65] There have in recent times, been developments which have to an

[59] See paras: 6.5.2 (Chapter 6); and 7.2.3.2(a) in Chapter 7.
[60] See Tladi supra n 26 191-2.
[61] See Buys supra n 15 160-4. The multi-layered approach aligns with international best practices see: paras 4.3.3 and 4.3.4 (ITU); para 4.4.2.2 and 4.4.2.3 (OECD); para 6.5.3 (USA) and paras 7.2.and 7.3 (Australia).
[62] See Ebersöhn (2004) supra n 26 142 where the author compares SA with USA and Australia; Tladi supra n 26 91 where the author compares SA with the USA; and Sibanda supra n 26 7-8 where Canada, the European Union, and South Africa are compared.
[63] Ebersöhn (2004) supra n 26 142.
[64] Ibid.
[65] See para 4.3.4.2 in Chapter 4.

extent addressed the criticisms identified above and also reflect on the solutions outlined. These are highlighted below.

8.2.6 Recent developments that shed light on the spam problem

These developments can be traced back to 2009 when the Internet Service Providers of South Africa[66] was formally recognized as an Industry representative Body (IRB) in terms of section 71 of the ECT Act.[67] ISPA was also at the forefront of the case in 2014 which required that the court interpret the provisions of section 45. In the discussion which follows, these developments – ie industry regulation and the section 45 provisions – are traced through case law.

8.2.6.1 Addressing section 45 criticisms through case law

(a) Introduction

In 2014 the first case dealing with the issue of spam namely: *Ketler Investment CC Presentations v Internet Service Providers' Association*[68] was heard before the courts. This case outlined the scope of the scourge that is spam, exposed the loopholes in section 45, and confirmed some of the criticisms levelled against that section. The case also highlighted the lengths to which ISPs go in order to protect themselves and their clients from receiving spam e-mails. Before getting into the discussion of these issues, the facts of the case will be briefly outlined so that when a discussion of the issues is highlighted below, it will be clear how the criticisms of section 45 were addressed in the case. Note should also be taken of the fact that the case is not discussed here at length but only those aspects related to the criticisms above are highlighted.[69]

[66] Hereafter 'ISPA'.

[67] See ISPA 'About ISPA' https://ispa.org.za/about-ispa (date of use: 20 January 2016). See ss 71 and 72 of the ECT Act for recognition of representative body; also Guidelines for Recognition of Industry Representative Bodies of Information System Providers (GN 1283 in *GG* 29474 of 14 December 2006), hereafter 'IRB Code'; Pistorius & Tladi supra n 26 700-03; and Marx & O'Brien (2011) 32/3 *Obiter* 551-6.

[68] See *Ketler Investment CC Presentations v Internet Service Providers' Association* 2014 (1) ALL SA 566 (GSJ), hereafter '*Ketler* case'.

[69] For a discussion of this case see Pistorius & Tladi supra n 26 688-705.

(b) *Ketler Investment CC Presentations v Internet Service Providers' Association*

The facts of the case are briefly that in 2012 the applicant (Ketler) engaged in the business of providing training courses throughout South Africa on the following matters: leadership; project management; and presentation skills.[70] The courses were marketed in a variety of ways, including by means of newsletters sent to consumers by e-mail. Although the applicant did not indicate whether it had created the e-mail address lists, or purchased or otherwise procured those from other sources, the promotional material was sent to the addresses on the list via bulk e-mail transmission. The e-mails were transmitted via an independent ISP to which Ketler subscribed.[71]

It came to the respondent's (ISPA) attention that Ketler had been sending unsolicited communications advertising its courses to consumers, even after those consumers had requested that it desist. The consumers also asked that the sender provide them with the source from which it had obtained their personal information. As a result of its spamming activities, ISPA listed Ketler as a spammer on its 'Hall of Shame' webpage.[72] The applicant then alleged that the respondent had defamed it by placing it on its hall of shame.[73] In coming to its decision, the court noted that:[74]

> the term "spammer", or a derivative, does not *per se* constitute defamatory matter. There is, however, a distinct insinuation to consumers using the Internet that the applicant is acting in at least a morally offensive manner at the consumers' cost. The terms "spam", "spammer", or "spamming", in the context of the overall contents of the respondent's hall of shame webpage, may also bear the connotation that the person referred to is acting in a manner abhorrent to the privacy rights of others. The court accordingly held that listing the applicant as a spammer in a hall of shame on the respondent's webpage, together with the wording of that webpage as a whole, was defamatory of the applicant in the secondary meaning.

[70] For the facts of the case see paras 1-3, 32-33 and 42-46 of the *Ketler* case supra n 68.

[71] For an example of the e-mail that the applicant sent to consumers see: id paras 36-38.

[72] The hall of shame is a webpage on ISPAs web site in which it lists spammers. See ISPA 'ISPA hall of shame' http://ispa.org.za/spam/hall-of-shame/ (date of use: 20 January 2016).

[73] See paras 2, 7 and 42-43 of the *Ketler* case supra n 68; and Pistorius & Tladi supra n 26 690-5.

[74] See id *Ketler* case paras 9, 44, 47, 50-5 and 55.

The court dismissed the application with costs,[75] and in 2014 Ketler paid ISPA an amount of R65 000.[76] In this instance it might well be said that the court succeeded in holding Ketler accountable for his spamming activities.[77]

(c) Lessons drawn from the case

Note should be taken here that apart from the issue of defamation, other issues were highlighted in the case. For a spammer to send e-mails the following are required: the list(s) of e-mails addresses of consumers (which might have been harvested or bought); the methods spammers use to send spam e-mails; the problems caused by such practices; the use of third party domain and e-mail addresses in order to remain undetected; and the efficiency of the opt-out mechanism; and counter-measures by ISPs to protect consumers and themselves from such practices. These issues are discussed below.

Section 45 does not outlaw spam

The *Ketler* case is a clear example of how spammers use the loophole in section 45 in order to advance their spamming activities. The applicant contended that "section 45(1) of the ECT Act doesn't prohibit spam but it does allow it to be sent in a regulated manner", and that the applicant had fully complied with the section.[78] Notably, Ketler continued sending spam e-mails although the recipients had requested them to stop. Although the applicant had provided a link or mechanism by which recipients could opt-out, clearly Ketler had no intention of honouring the requests. Section 45(1) not only encourages spammers to continue sending spam because they know they can, it also undermines recipients' confidence in the system.[79]

[75] Id para 105.

[76] Mybroadband 'SA spammer pays R65 000 to settle case' http://mybroadband.co.za/news/internet/104657-sa-spammer-pays-r65000-to-settle-case-case.html (date of use: 20 January 2016).

[77] In fact the ITU had noted that the most successful cases are those that have the opt-out mechanism as a default measure in combating spam (see para 4.3.4.2(c) (ii) in Chapter 4).

[78] See para 7(a) of the *Ketler* case supra n 68.

[79] Id para 59.

Disguising headers and spoofing

Another factor addressed in the *Ketler* case aimed at section 45 was that of the falsification of headers or spoofing.[80] ISPA established in this case that the applicant had used both third-party domains[81] and bogus e-mails to send spam. This explains why the consumers' requests were not honoured because the spammer was not in a position to process such requests.[82]

Harvesting and sale of lists

The issue of the harvesting or the sale of lists of e-mail addresses was also highlighted in the case but was left open as the court was unable to establish how the applicant had obtained the list(s) it used to send unsolicited communications to consumers. The applicant was not in a position to disclose or provide evidence of where it had received the lists of e-mail addresses.[83] The court, however, noted that lists can be harvested in a number of ways by those wishing to market their products or services through promotional material sent *en masse* by e-mail.[84]

The court acknowledged that the issue of harvesting was problematic, especially for well established businesses like banks. It also noted that harvesting amounts to "an impermissible invasion of privacy which lacks express and informed consent".[85] Confirming that this is a problem, it was recently reported that one of South Africa's cell phone providers had leaked its subscribers' personal information, a claim the cell phone giant denied.[86]

8.2.6.2 Self-regulation and the Internet Service Providers' Association (ISPA)

(a) Background

[80] Id paras 37-38 where an example of a spoofed e-mail is provided.

[81] Section 1 of the ECT Act defines a domain name as "alphanumeric designation that is registered or assigned in respect of an electronic address or other resource on the Internet".

[82] See para 32 of the *Ketler* case supra n 68.

[83] Id para 29 and Pistorius & Tladi supra n 26 699.

[84] Ibid. These lists can either be bought from third parties or harvested from other public sites.

[85] See para 29 *Ketler* case supra n 68.

[86] See Mochiko T 'Cybersecurity: oversharers anonymous' http://www.financialmail.co.za/features/ 014/11/06/cyber-security-overshares-anonymous (date of use: 20 January 2016).

ISPA was established in 1996 as a voluntary association and incorporated in 2016.[87] As a regulatory body, ISPA has a code of conduct with which its members must comply.[88]

(b) Anti-spam provisions in ISPA's Code

The ISPA code of conduct covers a variety of issues',[89] one being that of unsolicited communications (spam) in part F.[90] This clause prohibits ISPA members[91] from sending or promoting the sending of unsolicited electronic communications.[92] Members are also required to take reasonable measures to ensure that their networks are not used by others for that purpose.[93] Clause 17 urges members "to provide a facility for dealing with complaints regarding unsolicited electronic communications originating from their networks and, in addition, to react expeditiously to complaints received".[94] Note should be taken here that the ISPA code has an important element, namely, that the opt-out mechanism be attended to expeditiously,[95] which in itself aligns with the standards set by other jurisdictions such as the USA and Australia above.[96] In addition to the clauses above ISPA notes that all unsolicited bulk e-mail is spam with the following exceptions:[97]

> Mail sent by one party to another where there is already a prior relationship between the two parties and subject matter of the message(s) concerns that relationship, is not spam; mail sent by one party to another with the explicit consent of the receiving party, is not spam.

It is clear from the exceptions above that the ISPA make the sending of spam e-mails by its members' illegal. The above clauses favour an opt-in mechanism instead

[87] See ISPA 'About ISPA' supra n 67.

[88] See ISPA 'Code of conduct' http://ispa.org.za/code-of-conduct (date of use: 30 January 2016). Hereafter 'the ISPA Code'.

[89] The following are some issues contained in the ISPA Code: privacy and confidentiality (cl 4-5); consumer protection and provision of information to customers (cl 6-12); and cybercrime (cl 18).

[90] Id cls 16 and 17.

[91] See ISPA 'Membership' https://ispa.org.za/membership (date of use: 30 January 2016).

[92] Id cl 16.

[93] Ibid.

[94] Ibid.

[95] Ibid.

[96] See para 6.3.2.2 in Chapter 6; and 7.2.3.2 in Chapter 7.

[97] ISPA 'Spam' http://ispa.org.za/spam/ (date of use: 30 January 2016)

of the opt-out mechanism which is contrary to its mandate.[98] As a regulatory body ISPA was called out as applying double standards in its regulation of spam,[99] adding to earlier criticisms that this industry body was acting as both judge and jury in its regulation.[100]

(c) Technical measures by ISPA

The ISPA, like any other service provider, is affected by the activities of spammers, and this was highlighted in the *Ketler* case. The importance of technical measures by ISPs in limiting spam was also highlighted in the case as an attempt to establish who was sending the spam e-mails to consumers. The ISPA employed the following technical measures: the use of spam-trap address; and role of e-mail accounts in order to uncover who was behind the spam e-mails and why consumers were unable to opt-out of the unwanted e-mails.[101] These countermeasures cost resources for both the ISPs and consumers alike (although for consumers the impact is on a lesser scale).[102]

The fact that an industry body has been established (regardless of its problems, which it is hoped will be attended to in due course) has at least satisfied the suggestion above that there should be self-regulation in order to deal with the technical aspects of spam.

8.2.7 Conclusion

While South Africa broke ground regarding the issue of spam, especially at a time (2002 to be exact) when nations were implementing anti-spam laws and anti-spam provisions, note has to be taken that the provisions of section 45 are insufficient in regulating spam. In addition, recent developments have also confirmed the loopholes in those provisions and have intensified the problem as noted above. It is this authors view that section 45 as it currently reads does not even at a basic level

[98] Pistorius & Tladi supra n 26 700-03.
[99] Id 688-705.
[100] See Marx & O'Brien supra n 67 551-6.
[101] See para 57 of the *Ketler* case supra 68; Pistorius & Tladi supra n 26 698-700.
[102] Id *Ketler* case para 26-28 and 65-66; and id Pistorius & Tladi 698-9.

afford the required protection for consumers. Consequently, section 45, together with the attempts to make the provision more effective, have both created a band-aid solution which requires immediate attention. Hopefully, the other anti-spam and direct marketing provisions can shed light on the problem and perhaps offer better solutions than the ECT Act has to offer.

Below is a discussion of the provisions of the Consumer Protection Act and Protection of Personal Information Act. The discussion will also include selected provisions in the National Credit Act[103] where applicable.

8.3 Consumer Protection Act 68 of 2008

8.3.1 Background to the Consumer Protection Act

Before the adoption of the Consumer Protection Act[104] there were a number of pieces of legislation governing a variety of consumer issues'.[105] The CPA is the culmination of several decades of debate and legal development in the field of consumer protection in South Africa, involving the government, national and provincial legislatures, and academics.[106] The CPA "regulates the marketing of goods and services to consumers, plus relationships, transactions, and agreements between them and producers, suppliers, distributors, importers, retailers, and service providers of goods and services".[107] The CPA was signed into law on 24 April 2009 and came into effect on 31 March 2011.[108] The coming into operation of the CPA repealed some of the legislation which dealt with consumer issues, and made consequential amendments to various provisions in other Acts.[109]

[103] Hereafter the 'NCA'.

[104] Hereafter the 'CPA'.

[105] The following are examples: Business Names Act 27 of 1960; Merchandise Marks Act 17 of 1941; Price Control Act 25 of 1964; Sales and Service Matters Act 25 of 1964; Trade Practices Act 76 of 1976; and the Consumer Affairs (Unfair Business Practice) Act 71 of 1988.

[106] See McQuid-Mason et al *Consumer Law in South Africa* 385; Van Eeden *Consumer Protection Law* 23; De Stadler supra n 15 1-6; Naude & Eiselen *Commentary* 1-21; Woker (2010) 31/2 *Obiter* 217-23; and Du Preez (2009) 1 *TSAR* 58-83.

[107] Id Van Eeden 38-61; also id De Stadler 7-23; and id Naude & Eiselen 5.

[108] Consumer Protection Act 68 of 2008 (*GG* 32186 of 29 April 2009).

[109] Id s 121. The laws that were repealed include: s 2-13 and 16-17 of the Merchandise Marks Act 17 of 1941, and all the laws in n 105 above.

8.3.2 The purpose of the CPA

The purpose of the CPA is:[110]

> to establish a legal framework for the achievement and maintenance of a consumer market that is fair, accessible, efficient, sustainable, and responsible, and which promotes fair business practices. And which, moreover, protects consumers from unfair, unreasonable or otherwise improper practices from deceptive, misleading, unfair or fraudulent conduct, and improves consumer awareness and information and encourages responsible and informed consumer choice and behavior.

The CPA applies to transactions entered into or having an effect within the Republic which promote goods and services.[111] It also establishes a National Consumer Commission (NCC),[112] and entrenches the fundamental rights of consumers[113] – a first for South Africa.[114] Of importance to this part of work are consumer rights that involve anti-spam and direct marketing provisions. However, it should be noted that while there are a number of direct marketing provisions under the CPA,[115] only those that are housed in sections 11, 12, and regulation 4 of the CPA are outlined below. Part B of the CPA deals with the consumer's right to privacy which is discussed below.

[110] See s 3(1)(a); (c); (d); and (e) of the CPA.

[111] Id s 5(1)(a) and (b). See Van Eeden supra n 106 37-62 for the application and scope of the CPA and De Stadler supra n 15 24-56.

[112] See Chapter 5 of the CPA.

[113] See Jacobs, Stoop & Van Niekerk (2010) 13/3 *PELJ* 302-406; also De Stadler supra n 15 24-56; and Van Eeden supra n 106 25-55, for a general discussion of fundamental rights.

[114] See McQuid-Mason et al supra n 106 13-14; Van Eeden supra n 106 51-2; and Naude & Eiselen supra n 106 17-18. For an exhaustive list of these rights see: Chapter 2 parts A-H of the CPA which includes the following fundamental consumer rights: rights of equality in consumer market (Part A s 8-10); consumer's right to choose (Part C ss 13-21); right to disclosure and information (Part D sections 22-28); right to fair and honest dealing (Part F ss 40-47); right to fair, just and reasonable terms and conditions (Part G ss 48-52); right to fair value, good quality and safety (Part H s 53-61); and supplier's accountability to consumers (Part I s 62-67).

[115] For other provisions on direct marketing see the following sections: the consumer's right to cooling off period after direct marketing (s 16 of the CPA); also De Stadler supra n 15 32 and Van Eeden supra n 106 138-9); the consumers' right to return the goods (s 20 of the CPA; De Stadler supra n 15 34-6; and Van Eeden supra n 106 139); the right to fair and responsible marketing including among others: general standards for marketing of goods or services (s 29 of the CPA) and De Stadler supra n 15 60-1); bait marketing (s 30 of the CPA); also De Stadler supra n 15 78-9 and Van Eeden supra n 106 162); negative option marketing (s 31 of the CPA; also Naude & Eiselen supra n 106 para 31.1-31.4; De Stadler supra n 15 80; and Van Eeden supra n 106 163-4); direct marketing to consumers (s 32 of the CPA and De Stadler supra n 15 43); and catalogue marketing (s 33 of the CPA). For a discussion of these types of marketing see generally Opperman & Lake *Understanding the CPA* 23-64.

8.3.3 The consumer's right to privacy

The consumer's right to privacy is dealt with in section 11 of the CPA titled: "The right to restrict unwanted direct marketing". The section provides:

> (1) The right of every person to privacy includes the right to:
> (a) refuse to accept;
> (b) require another person to discontinue; or
> (c) in case of an approach other than in person, to pre-emptively block any approach or communication to that person, if the approach or communication is primarily for the purpose of direct marketing.
> (2) To facilitate the realisation of each consumer's right to privacy, and to enable consumers to efficiently protect themselves against the activities contemplated in subsection (1), a person who has been approached for the purpose of direct marketing may demand during or within a reasonable time after that communication that the person responsible for initiating the communication desist from initiating any further communication.
> (3) The Commission[116] may establish, or recognize as authoritative, a registry in which any person may register a pre-emptive block, either generally or for specific purposes, against any communication that is primarily for the purpose of direct marketing.
> (4) A person authorizing, directing or conducting any direct marketing-
> (a) Must implement appropriate procedures to facilitate the receipt of demands contemplated in subsection (2); and
> (b) Must not direct or permit any person associated with that activity to direct or deliver any communication for the purpose of direct marketing to a person who has:
> (i) Made a demand contemplated in subsection (2); or
> (ii) Registered a relevant pre-emptive block as contemplated in subsection (3).
> (5) No person may charge a consumer a fee for making a demand in terms of subsection (2) or registering a pre-emptive block as contemplated in subsection (3).
> (6) The Minister may prescribe regulations for the operation of the registry contemplated in subsection (3).

Section 12, on the other hand, deals with the regulation of the timeframes in which marketers may contact consumers[117] for marketing purposes. This section provides for a supplier[118] "not to engage in any direct marketing towards a consumer at home for any promotional purpose during a prohibited period – specific days, dates, public

[116] Section 1 of the CPA defines the term "Commission" as the "National Consumer Commission established in terms of s 85 of the CPA".

[117] Id s1 which defines the term "consumer" in respect of any particular goods and services as: "(a) a person to whom those particular goods and services are marketed in the ordinary course of the supplier's business; (b) a person who has entered into a transaction with a supplier in the ordinary course of the supplier's business, unless the transaction is exempt from the application of section 5(2) and 5(3). If the context so requires or permits, a user of those particular goods or a recipient or beneficiary of those particular services, irrespective of whether that user, recipient or beneficiary was a party to a transaction concerning the supply of those particular goods or services".

[118] Id s 1 where the term "supplier" is defined as: "a person who markets any goods or services".

holidays, or times of day – to the extent that the consumer has expressly or implicitly requested or agreed otherwise".[119]

8.3.4 Commentary on direct marketing provisions and the right to privacy under CPA

8.3.4.1 Definitions

Section 1 defines the term "direct marketing" as "to approach a person, (either in person,[120] by mail, or electronic communication), for the direct or indirect purpose of promoting or offering to supply, in the ordinary course of business, any goods;[121] or services;[122] or requesting the person to make a donation of any kind for any reason".[123] The term "electronic communications" is defined as 'communications by means of electronic transmission, including by telephone, fax, SMS, wireless computer access, e-mail or any similar technology or device'.[124] In recent years a number of cases have been decided confirming these means of communication as electronic communications.[125]

Hamann and Papadopoulos note that:[126]

[119] Id s 12(1) and (2) contrasted with s 75 of the NCA which deals with the harassment of consumers at home.

[120] The term "person" is defined as including "a juristic person in terms of s 1 of the CPA".

[121] The term "goods" is defined as including the following: "anything marketed for human consumption; any tangible object not otherwise contemplated in paragraph (a), including any medium on which anything is or may be written or encoded; any literature, music, photograph, motion picture, game, information, data, software, code or other intangible product written or encoded on any medium, or a licence to use any such intangible product; a legal interest in land or any other immovable property, other than an interest that falls within the definition of 'service' in this section; and gas, water and electricity" (ibid).

[122] The term "service" is defined as including, but is not limited to: "any work or undertaking performed by one person for the direct or indirect benefit of another; the provision of any education, information, advice, or consultation, except advice that is subject to regulation in terms of the Financial Advisory and Intermediary Services Act 37 2002; and any banking services or related or similar financial services, or the undertaking, underwriting or assumption of any risk by one person on behalf of another" (ibid).

[123] Ibid.

[124] Ibid.

[125] See the following cases: *Jafta v Ezemvelo KZN Wildlife* (2009) 30 ILJ 131 (LC), where it was decided that an SMS was an electronic communication; also *Sihlali v South African Broadcasting Corporation Ltd* [2010] ZALC 1, (2010) 31 ILJ 1477 (LC); and *Spring Forest Trading v Wilberry (Pty) Ltd t/a Ecowash Combined Motor Holdings Limited* (725/13) [2014] ZASCA 178, 2015 (2) SA 118 (SCA).

[126] See Hamann & Papadopoulos supra n 26 54; and De Stadler supra n 15 63.

> the CPA's protection granted to consumers differs slightly from that of the ECT Act's section 45, … protection is granted for direct marketing via an electronic communication, as well as requests for donations of any kind, whereas the ECT Acts relates only to UCE.

This definition also accommodates the concern raised above that other types of spam are not included in the UCE, for example, by including "requests for donations of any kind". The Act does not define the term donation, but one would assume that should a charity organisation or public institution request a gift or free contribution from consumers that would constitute spam.[127]

8.3.4.2 Direct marketing and the right to privacy

There is a relationship between direct marketing and the right to privacy. Some have noted that direct marketing involves two possible infringements of the right to privacy: firstly, when private information is gathered by the direct marketer without the knowledge of the consumer; and secondly, where consumers are contacted without their consent.[128] Direct marketing may also be sent to consumers without aiming the marketing at consumers individually.[129]

Under the CPA the right to privacy is noted as a right to be left alone, and also cover what others refer to as "information privacy".[130] Roos notes that "while the CPA provides no comprehensive regulation of information privacy, it does regulate information privacy only when the person can be contacted, but disregards how the direct marketer came to possess the contact details in the first place".[131] Some note

[127] See Merriam Webster 'Donation' https://www.merriam-webster.com/disctionary/donation (date of use: 6 March 2017).

[128] See Naude & Eiselen supra n 106 11.9.

[129] Id para 11.13. On the other hand the term "advertisement" is defined in s 1 of the CPA as "any direct or indirect visual or oral communication transmitted by any medium, or any representation or reference written, inscribed, recorded, encoded upon or embedded within a medium, by means of which a person seeks to: bring to the attention of all or part of the public, the existence or identity of a supplier; or the existence, nature, availability, properties, advantages or uses of any goods or services that are available for supply, or the conditions on, or prices at which any goods or services are available for supply; promote the supply of any goods or services; or promote any cause".

[130] See s 11(1)(a) of the CPA; also Naude and Eiselen supra n 106 11.8; 11.9; De Stadler supra n 15 28; and Van Eeden supra n 106 128-9. Information privacy is regulated by the Protection of Personal Information Act, 2013.

[131] See Roos 'Data privacy law' 432-4. De Villiers notes that "the CPA thus prohibits the use of, or permitting a sender to use, a recipient's personal information for promotional purposes unless the recipient has consented to his or her information being used in that way" (see De Villiers (2007) Oct/Nov *Journal of Marketing* 19).

that to develop this marketing relationship consumers "must perceive the benefits derived from the relationship with the marketer as outweighing the costs/disadvantages".[132] South Africans are largely ignorant when it comes to information privacy (data protection) and freely reveal such information in the context of their shopping experience, especially when engaging with direct marketers.[133] By so doing, their personal information remains in the possession of the marketer who may either abuse or misuse it to the consumer's detriment.[134] While it is important to note that there can be no transaction or exchange without the communication of information, consumers still lag behind when it comes to enforcing their rights. Some note that "as a minimum, the two parties must be aware of one another's existence,[135] and must have some idea of what will be exchanged and what the respective benefits may be".[136]

8.3.4.3 Opt-out mechanism

Section 11 allows for direct marketing to be sent by placing a duty on the consumer to do something about it. In this case the consumer can exercise his or her right to privacy by refusing to accept such marketing material, or requiring another person to discontinue or pre-emptively block such advances.[137] This provision brings the opt-out mechanism into play. Section 11(2) provides for a direct marketer to desist from sending unsolicited communications within a reasonable time when a request has been made by the consumer. In addition, section 11(4) places an obligation on the senders to "implement appropriate procedures" to facilitate the receipt of demands contemplated in subsection 2.[138] These appropriate measures will be to act within a reasonable time upon receiving such demand. This subsection prohibits the sender

[132] See Jordaan & Jordaan (2004) 23/1 *Journal for Communication Sciences in Southern Africa* 139.

[133] See Jordaan (2007) 3/1 *International Retail and Marketing Review* 45; Naude & Eiselen *Commentary* supra n 106 para 11.9.

[134] Ibid.

[135] See Jordaan & Jordaan supra n 132 139.

[136] Ibid.

[137] See s 11(1) of the CPA. Contrast this with s 74(6) of the NCA which provides for: "the credit provider to present the consumer with a statement of options and afford the recipient an opportunity to choose to be excluded from any telemarketing campaign that may be conducted by or on behalf of the credit provider. The credit provider must also maintain a register of all options selected by consumers in the prescribed manner and form, and that the credit provider must not act contrary to an option selected by a consumer" (see s 74(7)(a) and (b) of the NCA).

[138] See s 11(4)(a) of CPA.

to direct or permit a third party or persons associated with the direct marketing activities to direct or deliver communications to consumers who have made a demand in subsection 2; and or have registered "a relevant pre-emptive block".[139] This provision and that dealing with the pre-emptive block are also consistent with anti-spam provisions in other jurisdictions.[140] Section 11 provisions are consistent with section 45(1) (a) of the ECT Act as outlined above with regard to the provision of an opt-out mechanism. But unlike the ECT Act, the CPA goes a step further addressing when the demands should be attended to.[141] Although the CPA makes provision for the consumer to demand that communication desist within a reasonable time after initiation, it, however, fails to expand on what those time frames are. The phrase "within reasonable time" is relative, as it means different things to people, for some it might mean the moment the demand enters the spammers/senders e-mail box, and for others, anytime when the spammer/senders decides to open such email even if they might have received such demands earlier. Also this will only be effective in cases where the sender has provided accurate sender information or have not disguised their headers, a provision not made for in the CPA and which has an impact on the "appropriate measure" provision.

Section 11 presupposes that the marketer will always make him- or herself known to the consumer and not falsify his or her headers.[142] It also fails to provide that the opt-out facility should be operational for a prescribed period so as to enable the sender to make use of it.[143] The CPA also makes provision for recipients to opt-out of unsolicited e-mails without having to pay for such a service.[144] This is not so much of a problem regarding online spam but it is problematic with regards to mobile spam, where consumers are constantly being asked to pay a fee to opt-out of such communications.[145] Overall, the provisions of CPA regarding the opt-out facility are a

[139] Ibid s 11(4)(b) read with 11(3) and (6). See Naude & Eiselen supra n 106 paras 11.16-11.17; and Van Eeden supra n 106 130.

[140] See the following paragraphs in Chapters 6 and 7 above: 6.3.2.2 (c) (USA which covers the prohibition of transmission after objection); and 7.2.3.2 (c) (Australia which provides for a functional unsubscribe facility).

[141] See s 11(4) read with (2) of the CPA.

[142] See Hamann & Papadopoulos supra n 26 54-5.

[143] Ibid.

[144] Section 11(5) of the CPA; and Naude & Eiselen supra n 106 paras 11.18-11.19.

[145] See Mybraodband 'Spam SMS: why South Africans pay to reply 'stop'' https://mybroadband.co.za/news/smartphones/136828-spam-sms-why-south-africans-pay-to-reply-stop.html (date of use: 6 March 2017).

step forward on the ECT Act by putting additional measures in place to protect consumers. The CPA provisions are also lacking in some areas – for example, there are no provisions on falsifying sender information or spoofing, or timeframes on how and when the opt-out should be facilitated, et cetera. Perhaps the answer lies in the pre-emptive block which the consumer can utilise to stop communications even before he or she has been approached.

8.3.4.4 National do-not-call registry

(a) Background

The CPA provides for the consumer to pre-emptively block any approach either in person or via a communication sent, if that approach is mainly for purposes of direct marketing.[146] Section 11(3) of the CPA provides for a registry to be established by the Commission, or that an "authoritative registry" be recognised on which any person may register a pre-emptive block against direct marketing communications.[147] Section 11(6) provides for the Minister to issue regulations for the operation of the registry.

(b) Regulation 4: Mechanisms to block direct marketing communications

Regulation 4 deals with the mechanism to block direct marketing communications, and covers a number of issues including the administration of the pre-emptive block and minimum requirements for the operation of the registry. Regulation 4(3) sets out the following requirements as minimum for operating the registry as contemplated in section 11(3):[148]

> (a) The registry must be capable of accommodating all persons in the Republic and cover the whole geographical area of the Republic;
> (b) The registry must at all times be accessible to all persons in the Republic for purposes of registering a pre-emptive block, without payment of any fees, but the person registering must pay the actual cost of the type of communication available for registration;
> (c) A consumer may register-
> (i) His or her name, identification number, passport number, telephone number, cell phone number, facsimile number, e-mail address, postal address, physical address, a

[146] See ss 11 (1)(c) and 11(4)(b) of the CPA.
[147] Id s 11(3).
[148] See reg 4(3) of the CPA.

> web site uniform resource locator ("URL") or any other identifier which the operator of the registry makes provision for;
>
> (ii) The consumer's own global address for any web site or web application or the site on the world wide web;
>
> (iii) If the operator of a registry so allows, the pre-emptive block for any time of the day or any day of the year; or
>
> (iv) If the operator of the registry so allows, a comprehensive prohibition for any medium of communication, address or time whatsoever.
>
> (d) Any pre-emptive block registered in accordance with this regulation becomes effective 30 days from the date on which it is registered.

Once a register has been compiled the direct marketer can make an application to the administrator[149] of the registry to confirm whether or not a pre-emptive block has been registered by a specific consumer.[150] The administrator may not provide the marketer with any details regarding any identifiable information of the consumer provided to the registry.[151] An exception will be if the direct marketer has proof that an existing client has, after the commencement of the regulations, expressly consented to receiving direct marketing from marketers themselves.[152]

In addition to the minimum requirements set out above, reg 4 also makes provision for the harvesting and sale of lists, a provision not covered under the ECT Act.[153] Sub-regulation 4(e) prohibits the administrator of the registry "from providing, selling, or otherwise disposing of any information contemplated in sub-regulation (c) to anyone – including any organ of state – save with the express, written permission of the consumer concerned, or by order of a court of law, or by operation of law".[154] Regulation 4(4) also provides for the administrator to:[155]

> proactively put in place sufficient security arrangements to prevent the manipulation, theft, or loss of data in the registry; compliance with any law for the protection of personal information or the protection of privacy; and also, from time to time in all official languages, conduct public information campaigns as required and approved by the Commission.

The provision for the harvesting and sale of lists is consistent with the provisions in the USA and Australia above, save that the CPA does not provide for the use of

[149] Id regs 4(3)(e), (f), (h), (l), and 4(4). For a discussion of the administrator: see Van Eeden supra n 106 129-34; Naude & Eiselen supra n 106 paras 11.18-11.11.19; and De Stadler supra n 15 62-6.

[150] Id reg 4(3)(g).

[151] Id reg 4(3)(f).

[152] Ibid.

[153] Id reg 4(3)(e).

[154] Ibid.

[155] Id reg 4(4)(a); (b); (c) and (d).

software to harvest those lists. It should be noted that the CPA follows in the footsteps of the CAN-SPAM's Act above, in that it calls for the establishment and implementation of the registry.[156] It remains to be seen whether the registry as contemplated in the CPA will be implemented by the Minister years after the CPA has come into operation.[157] The implementation of the do-not-contact list was put out on tender as early as 2011,[158] followed by another attempt in 2013.[159] At that time there were only two responses to the call for applications to administer such a registry.[160] At the time of writing (January 2017) the registry has still not been established. However, there is a registry administered by the Direct Marketing Association of South Africa[161] in place.

(c) DMASA and its competitors

Direct marketers rely on their databases in order to communicate with customers. Most direct marketing activities flow from an organisation's database which contains valuable consumer information.[162] In 2005 the DMASA was established as an association of direct marketing companies aimed at "protecting both industry and consumers from unethical or ignorant practitioners, and to lobby government and other regulatory bodies".[163]

[156] See Chapter 6 para 6.3.2.5 above. Also see the Australian version: ADMA 'Do not mail-consumers' https://www.adma.com/au/do-not-mail (date of use: 20 January 2016); and ACMA 'Do not call register' https://www.donotcall.gov.au (date of use: 20 January 2016).

[157] See Naude & Eiselen supra n 106 paras 11.18-11.19 and Van Eeden supra n 106 129-33.

[158] See GN 129 of 2011 *GG* 34088 of 8 March 2011. Also see TouchBasePro 'Impact of the Consumer Protection Act on your e-mail marketing' 6 http://creative engineeringstudio.com/wp-content/uploads/2015/06/Impact-of-the-Consumer-Protection-Act-on-your-Email-Marketing_TouchBasePro_May2011.pdf (date of use: 20 January 2016); Mawson N 'No decision on opt-out registry yet' http://www.itweb.co.za/index.php?option=comcontent&view=article&id=47451 (date of use: 28 January 2016).

[159] See Mawson N 'Finally, a national opt-out list' http://www.itweb.co.za/index.php?id=69237 (date of use: 28 January 2016).

[160] Ibid.

[161] Hereafter 'DMASA'. See DMASA 'DMASA Direct Marketing Association' http://www.dmasa.org/home/about-us (date of use: 20 January 2016).

[162] See Jordaan (2007) supra n 133 43.

[163] The DMASA seeks to regulate and professionalise the direct marketing trade by fostering trust, honesty, and accountability within the industry. See DMASA 'DMASA Direct Marketing Association' supra n 161. See Mudelair (2008) *Journal of Marketing* 22; and Naude & Eiselen supra n 106 11-13.

Key to the DMASA's activities is the promotion and expansion of interactive and direct marketing within the country and region.[164] Since 2007 the DMASA has been administering a national do-not-call registry (opt-out registry).[165] This registry is a web site where consumers provide their personal details to pre-empt marketers from sending unwanted e-mails.[166] Once the consumer is registered, he or she can also amend their particulars when necessary so linking to the existing contact details that can be modified.[167] According to the then CEO of the DMASA "some marketers were completely ignorant of the practice of verifying the database before contacting consumers which meant that consumers were anyway consulted".[168] The DMASA members can access the registry free of charge to make use of its database list, as can non-members but subject to a fee.[169]

In 2011 it was reported that the personal information of some 39 000 consumers registered on the DMASA site had been leaked to companies that were not DMASA members.[170] Different views have been offered by those who had registered ranging from "the system being ineffective as they continue to receive unsolicited e-mails' and that their personal information is also circulated outside the DMASA which is against the rules of that association".[171]

In 2012 it was reported that in the five years after its inception, the DMASA had registered 70 000 consumers who opted not to receive marketing from DMASA

[164] DMASA offers a hotline to both consumers and competitors for complaints and it seeks to resolve issues through arbitration. DMASA is also an active member of the Advertising Standards Authority. Ibid DMASA.

[165] See Direct Marketing Associating of SA 'The DMA National OPT OUT Database' https://www.nationaloptout.co.za (date of use: 28 January 2016).

[166] Ibid. The requirements of registration on this site are: to provide: a valid RSA ID number and e-mail address or cell number; contact details that they wish not to be contacted. On completion of the registration once the submit button has been clicked, the consumer will receive an e-mail requesting that they confirm their wish to be on the national opt-out database. Once confirmation has been received the consumer will be registered. If however, the consumer does not reply in five days then their details will be deleted. It takes six weeks for this service to be fully effective for example, for all members of the DMASA to stop contacting consumers.

[167] See Direct Marketing Associating of SA 'The DMA National OPT OUT Database' supra n 165. The changes to the consumer profile can be done on the DMASA site.

[168] Mudelair supra n 163 22.

[169] Id 23.

[170] See Mawson N 'DMASA database 'leaked'' http://www.itweb.co.za/index.php?option=com_content&view=article&id=44060:dmasa-database-leaked&utm_source=Story&utm_medium=Web&utm_term=44060:dmasa-database-leaked&utm_content=44060:dmasa-database-leaked&utm_campaign (date of use: 28 January 2016).

[171] Ibid.

associates.[172] This lack of growth was attributed to the fact that the public might not be aware (lack of education) of such a registry, or that consumers were afraid to enter their personal information on the registry because they were uncertain of where that information might end up.[173] Swales note:[174]

> The National Consumer Commission ought to have established a better ‘do-not-contact’ system in terms of the provisions of s 11 of the CPA. Although it is laudable that the DMASA has established its own opt-out database, it also suffers from the issues all self-regulatory bodies are plagued with enforcement and compliance.

Apart from the DMASA there is another opt-out registry administered by TrustFabric. TrustFabric is a company that builds vendor relationship management software.[175] TrustFabric also creates a platform which allows individuals to keep their personal information up-to-date in one place, and then, selectively and securely, to share that information with organisations with whom they have relationships.[176] In 2012 it was reported that TrustFabric had registered 70 000 individuals in its do-not-contact registry within ten days of its establishment.[177] TrustFabric also noted that consumers who wrote to the NCC expressed their concern about the conflict of interest arising from the DMASA having control over managing the national opt-out list.[178]

In 2014 it was reported that there were less than 400 000 consumers who had signed up on both TrustFabric’s and DMASA’s registries.[179] Both DMASA and TrustFabric were named as the two associations that were interested in administrating the opt-out registry in that year. It has been estimated that the cost of establishing an opt-out service will be in the order of five million Rand – a possible reason for the registry not having yet materialised.[180]

[172] Mybroadband ‘Spam opt-out lists: TrustFabric versus DMASA’ http://mybroadband.co.za/news/general/47560-spam-opt-out-trustfabric-versus-dmasa.html (date of use: 20 January 2016).
[173] Ibid. Also Mawson N ‘No decision on opt-out registry yet’ supra n 158.
[174] Swales supra n 26 75.
[175] See TrustFabric ‘About us’ https://www.trustfabric.com/about (date of use: 28 January 2016).
[176] Ibid.
[177] See Mybroadband. ‘Spam opt-out lists: TrustFabric versus DMASA’ supra n 172.
[178] Ibid.
[179] See Mawson N ‘DMASA database ‘leaked’’ supra n 170.
[180] Ibid.

8.3.4.5 Enforcement

Section 4(1) of the CPA deals with the realisation of consumer rights and provides individuals[181] with a number of options should they feel aggrieved. Individuals can approach a court, the Tribunal,[182] or the NCC,[183] if their consumer rights have been infringed, impaired, or threatened, or if prohibited conduct has taken place.[184] The NCC can also initiate a complaint of its own accord, and also investigate complaints by consumers after which the matter will either be resolved by the NCC or be passed on to the National Credit Tribunal (NCT) for adjudication.[185] If the supplier concerned is an industry not regulated by an ombudsman, the claim can be referred to a provincial consumer court,[186] an alternative dispute resolution agent,[187] or the NCC.[188]

The Commission may also cooperate with, facilitate, or otherwise support the activities carried out by a consumer protection group which include:[189] consumer advice and education activities and publications; research, market monitoring, surveillance and reporting; promotion of consumer rights; and advocacy of consumer interests.

[181] Section 1 of the CPA defines the term "individuals" as including the following: "a person acting on his or her own behalf; an authorised person acting on behalf of another person who cannot act in his or her own name; a person acting as a member of or in the interest of a group or class of affected persons; a person acting in the public interest, with leave of Tribunal or court as the case may be; and an association acting in the interest of its members".

[182] Id s 4(2)(a) provides that: "in any matter brought before the Tribunal or a court in terms of the Act: (a) the court must develop the common law as necessary to improve the realisation and enjoyment of consumer rights generally and in particular by persons contemplated in s 3(1)(b)"; s 4(2)(b) provides that "the Tribunal or court as the case may be: to promote the spirit and purposes of the Act; and make appropriate orders to give practical effect to the consumers right to access to redress including but not limited to: any order provided for in the Act; and any innovative order that better advances, protects, promotes and assures the realisation by consumers of their rights in terms of the Act". See De Stadler supra n 15 169-71 and Opperman & Lake supra n 115 205-12.

[183] Id s 71(2). The section provides for any person to file a complaint concerning a matter with the Commission in the prescribed manner or form alleging that a person has acted in a manner inconsistent with this Act.

[184] Id s 4(1).

[185] De Stadler supra n 15 175-80; and Magaqa (2015) 27/1 *SA Merc LJ* 32-57 for a discussion of the NCC and NCT.

[186] See s 76 of the CPA; Opperman & Lake supra n 115 223-224; and De Stadler supra n 15 173-5.

[187] Id s 70; and De Stadler supra n 15 171-2.

[188] See Chapter 5 of the CPA for the National Consumer Protection Institutions and s 99-101 for the enforcement functions of the NCC, compliance notices and objection to notices. Also see De Stadler supra n 15 175-80 for a discussion of the investigations of the NCC; Opperman & Lake supra n 115 208-12; and Naude & Eiselen supra n 106 para 83.1- 84.2 and 99.3-99.8.

[189] See s 77-78 and 84(a)-(e) of the CPA and Opperman & Lake supra n 115 230-6.

8.3.4.6 Penalties

Any person convicted of an offence in terms of the CPA is liable[190] to a fine or to imprisonment for a period not exceeding ten years, or to both a fine and imprisonment.[191] The magistrate's court has jurisdiction to impose any penalty provided for in section 111(2) of the CPA.[192]

8.3.5 Conclusion

As noted above, the CPA has made provision for the requirements of sending direct marketing communications and advances which to an extent are in accord with international best practices as contrasted with those in other jurisdictions. The issue of the registry remains problematic as it creates uncertainty among consumers who are unable to exercise their rights as provided for in the Act.

This uncertainty leaves consumers in a vulnerable place and direct marketers will inevitably exploit the situation. Overall, the provisions on direct marketing have been noted as "a welcome relief that is long overdue, as [they give] the consumer the right to reject and or accept unsolicited communications".[193]

The last anti-spam or direct marketing provisions to be considered are those in the Protection of Personal Information Act. An examination of these is outlined with a view to establishing whether they will bring us any closer to properly regulating spam, or whether they will, in fact, complicate the issue.

8.4 Protection of Personal Information Act 4 of 2013

8.4.1 Background to the Protection of Personal Information Act

[190] Id s 111(1)(a)

[191] Id s 107(1) which deals with the breach of confidence and provides for an offence for those disclosing any personal information or confidential information concerning the affairs of any person obtained: (a) in the carrying out any function in terms of this Act; and (b) as a result of initiating a complaint or participating in any proceedings in terms of this Act. See exceptions to the above in s 107(2) of the CPA.

[192] Id s 111(2). For costs and offences related to prohibited conduct see s 108-110 and 112-113; Opperman & Lake supra n 115 237-41; and Naude & Eiselen supra n 106 para 99.1-99.2.

[193] See Papadopoulos supra n 15 235; and Hamann & Papadopoulos supra n 26 53-4.

The protection of personal information, or data protection, provides legal protection for a person in instances where his or her personal information is processed by another person or an institution.[194] This concept has also been interpreted to include the legal, regulatory, and institutional mechanisms that guide the collection, use, and disclosure of information.[195] While other jurisdictions have been regulating the personal information of its citizens for decades, South Africa has only recently moved in this direction.[196]

The forerunner to the Protection of Personal Information Act[197] was a discussion paper tabled before the South African Law Reform Commission.[198] The topic 'Privacy and Data Protection' was considered by the Commission as far back as 2005 in a discussion paper which contained a draft Bill on the protection of personal information.[199] In 2009 the POPI Bill was drafted, and in November 2013 the POPI Act was approved, signed into law, and published in the *Government Gazette* on 26 November 2013.[200] The POPI Act has been dubbed 'South Africa's EU-style data protection law' by some.[201] There has been a need for this type of legislation in

[194] See Neethling, Potgieter & Visser *Neethling's Law of Personality* 267-81.

[195] The term "data protection" is commonly used in the following jurisdictions, among others, the United Kingdom and the European Union. In South Africa it is referred to as the 'protection of personal information'. Id 267; and Roos 'Data privacy law' 368.

[196] See Neethling (2012) 75 *THRHR* 242 where the author notes that "there are 76 countries that have introduced data protection laws". For a discussion of these data protection laws see the following works: Naude and Papadopoulos (2016) 79/2 THRHR 214-226; and Papadopoulos & Snail 'Privacy and data protection' supra n 23 295-7 discussing the USA, OECD, and EU data protection rules; Id Roos 370-416 discussing the OECD guidelines, the Council of Europe Convention on Data Protection, and international data codes such as the United Nations, the Asia-Pacific Economic Cooperation, and African initiatives; Roos (2008) 4 *PELJ* 62-109; Roos (2007) 124/2 *SALJ* 400-3; and Van Schalkwyk & Marlie *The protection of commercial information in electronic communications* 38/1 46-72 and 87-90 for a discussion of the EU and the UN Guidelines.

[197] Hereafter 'POPI Act'.

[198] See South African Law Reform Commission (SALRC) Discussion Paper 109 Project 124 *Privacy and Data Protection* (2005). See also Maheep supra n 26 30-3; and Naude & Papadopoulos (2016) 79/1 51-52.

[199] See the following works discussing the Draft POPI Bill: Neethling supra n 196 245-255; also Roos 'Data privacy law' 434; Roos 'Data protection' 367-389; Papadopoulos & Snail supra n 23 299-309; Hamman & Papadopoulos supra n 26 55-7; and Papadopoulos supra n 15 230-2.

[200] See Protection of Personal Information Act 4 2013. This Act is the first South African legislation that fully protects the processing of personal information of data subjects. See Michaelson 'POPI signed by the President' http://www.michaelson.co.za/blog/popi-signed-by-the-president/12625 (date of use: 20 January 2016).

[201] See Stein (2012) 12/10 *Without Prejudice* 48-9; Monty (2015) 15/6 *Without Prejudice* 86-7; and Matthes C 'Unpacking the POPI Act: The ins and outs of protecting personal information' http://www.itweb.co.za/index.php?option=com_content&view=article&id=71001 (date of use: 28 January 2016).

South Africa for decades, and it is encouraging that it is now finally in place.[202] It must be noted, however, that the operation of the POPI Act is to be introduced piecemeal by proclamation in the *Government Gazette.*

8.4.2 The purpose of the POPI Act

The aim of the POPI Act is to give effect to the constitutional right to privacy[203] by safeguarding personal information when processed by a responsible party, subject to justifiable limitations aimed at balancing the right to privacy against other rights, in particular, the right of access to information.[204] The POPI Act also protects important interests, including the free flow of information within the Republic and across international borders.[205]

The POPI Act provides persons with rights and remedies to protect their personal information from processing that is not in accordance with the Act.[206] It also establishes voluntary and compulsory measures – including the office of the Information Regulator who exercises powers and performs duties and functions in terms of the Act.[207] The Act applies to fully, partly,[208] and to the non-automated processing of personal information.[209]

The POPI Act does not apply to the processing of personal information in the course of a purely personal or household activity,[210] or to information that has been de-

[202] See Neethling supra n 196 241-2; also Roos *Data Protection* 654; and McQuoid-Mason (1982) XV/1 *CILSA* 135.

[203] The right to privacy is one of the fundamental human rights protected by the Constitution of South Africa Act 108 of 1996. Section 14 of the Constitution states that: “everyone has the right to privacy, which includes the right not to have the privacy of their communications infringed”. For a discussion of the right to privacy and common law see Roos ‘Data privacy law’ 418-22; Naude & Papadopoulos supra n 198 52-6; Neethling supra n 196 243-4; Papadopoulos & Snail supra n 23 276-8; Van Schalkwyk & Marlie supra n 196 75-6; Neethling, Potgieter & Visser supra n 194 217-54 and 370-3; Hofman *Cyberlaw* 43-62; Goodburn & Ngoye supra n 23 171-96; and Buys ‘Privacy and the right to information’ 365-91.

[204] See s 2(a)(i) of the POPI Act.

[205] Id s 2(a)(ii).

[206] Id s 2(c).

[207] Id s 2(d). Chapter 5 of the POPI Act deals with supervision by the Information Regulator.

[208] Id s 2(4). The term automated is defined in s 1 of the POPI Act as meaning “equipment capable of operating automatically in response to instructions given for the purpose of processing information”.

[209] Id s 3(1)(a).

[210] Id s 6(1)(a). This covers the area where one keeps a directory of telephone numbers and addresses of friends and acquaintances. See Roos ‘Data privacy law’ 439.

identified to the extent that it cannot be re-identified.[211] Section 5 of the POPI Act addresses the rights of data subjects.[212] The POPI Act also regulates how personal information may be processed by setting conditions, in line with international standards, which prescribe the minimum threshold requirements for the lawful processing of personal information.[213] The conditions for lawful processing of personal information include: the collection; purpose; use; quality; security; and the accountability of organisations in relation to that personal information.[214] These information principles will not be discussed in depth here but certain conditions will be outlined in the discussion on unsolicited communications below.

8.4.3 Direct marketing and unsolicited communications under the POPI Act

8.4.3.1 Section 69: The rights of data subjects regarding direct marketing by means of unsolicited electronic communications, directories and automated decision making

Section 69 provides:

> (1) The processing of personal information of a data subject for the purpose of direct marketing by means of any form of electronic communications, including automated calling machines, facsimile machines, SMSs or e-mail is prohibited unless the data subject:
> (a) Has given his, her or its consent to the processing; or
> (b) Is, subject to subsection (3), a customer of the responsible party.
> (2) (a) A responsible party may approach a data subject:
> (i) Whose consent is required in terms of subsection (1)(a); and
> (ii) Who has not previously withheld such consent only once in order to request the consent of the data subject.
> (b)The data subjects consent must be done in a prescribed form.
> (3) A responsible party may only process the personal information of a data subject who is a customer of that responsible party in terms of subsection (1) (b):
> (a) If the responsible party has obtained the contact details of the data subject in the context of a sale of product or services;
> (b) For purposes of direct marketing of the responsible party's own similar products or services; and

[211] Id s 6(1)(b).

[212] Id s 5(a)-(i). These include the right to have the data subjects' personal information processed in accordance with the conditions for the lawful processing of personal information. See Roos 'Data privacy law' 464-5.

[213] Id s 4.

[214] These information protection principles (conditions for lawful processing) are covered in Chapter 3 of the POPI Act. For a discussion of these principles see the following: Swales supra n 26 61-5; Roos 'Data privacy law' 442-54; Maheep supra n 26 44-50; Neethling supra n 196 247-54; Papadopoulos & Snail supra n 23 301-305; Roos 'Data Protection' 371-9; Roos (2006) 39/1 *CILSA* 107-27; Neethling, Potgieter & Visser supra n 194 267-81; and Van Schalkwyk & Marlie supra n 196 72 and 87-90.

(c) The data subject must also be given reasonable opportunity to object free of charge and in any manner free of unnecessary formality, to such use of his, her or its electronic details-
    (i) At the time when the information is collected; and
    (ii) On the occasion of each communication with the data subject for the purpose of marketing if the data subject has not initially refused such use.

(4) Any communication for the purpose of direct marketing must contain:
    (a) Details of the identity of the sender or the person on whose behalf the communication has been sent; and
    (b) An address or other contact details to which the recipient may send a request that such communication cease.

8.4.3.2 Commentary on direct marketing and unsolicited communications under the POPI Act

(a) Definitions

Section 1 of the POPI Act defines direct marketing as:

> approaching a data subject, either in person or by mail or electronic communication for the direct or indirect purpose of: (a) promoting or offering to supply, in the ordinary course of business, any goods or services to the person; or (b) requesting the person to make a donation of any kind for any reason.

At the outset it is important to note that the definition of direct marketing under the POPI Act corresponds to that in the CPA, save for a difference in the terms "data subject"[215] and "consumer". Some note that "direct marketing includes the collection of data using software and cookies which are also data files, but are not protected under the automated decision-making provisions in that legal consequences do not necessarily attach to them".[216] Section 69(1) provides for direct marketing as covering the processing of data subjects' personal information[217] in the following mediums: automatic calling machines;[218] facsimile; SMSs; or e-mail.[219] These

[215] Id s 1 defines "data subject" as "the person to whom personal information relates".

[216] Hamann & Papadopoulos supra n 26 59.

[217] Ibid. This section defines the term "personal information" as "information relating to an identifiable, living, natural person and where it is applicable, an identifiable, existing juristic person, including but not limited to: information relating to race, gender, sex, age et cetera; information relating to the education or the medical financial criminal or employment history of a person; any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other particular assignment to the person; the biometric information of the person; and the name of a person if it appears with other personal information relating to the person or if the disclosure of the name itself would reveal information about the person".

[218] See s 69(5) which defines "automated calling machines" as "a machine that is able to make automated calls without human intervention".

[219] Id s 69(1); and Roos 'Data privacy law' 460-1.

mediums correspond to those covered by the definition of electronic communications under the CPA. The term electronic communications, on the other hand, is defined as "any text, voice, sound, or image message sent over an electronic communication network which is stored in the network or in the recipients' terminal equipment until he or she collects it".[220]

Roos notes that a major requirement in the POPI Act is that "the information must have been obtained in the context of a sale, which links unsolicited communications with the "content" element which is "commercial", rather than with the bulk or volume of the message".[221]

(b) Opt-in mechanism

Section 69(2) provides for the responsible party[222] to request for consent before they can send unsolicited communications, and also that the data subject must not have withheld such consent.[223] The responsible party must approach the data subject once to request such consent. The term "consent" is defined as "any *voluntary*, *specific*, and *informed expression* of will in terms of which permission is given for the processing[224] of personal information". The number of times the term "consent" features in the section including other terms used to describe that consent emphasizes the importance and intensity of the provision. Although those descriptors are not defined it is clear that the person giving the consent must have done that

[220] Id s 1.

[221] Id ss 69-70; and Roos 'Data privacy law' 461-62.

[222] Ibid s 1 defines the term "responsible person" as meaning "a public or private body or any other person which, alone or in conjunction with others determines the purpose of and means for processing personal information. A private body on the other hand means: a natural person who carries or has carried on any trade, business or profession, but only in such capacity; a partnership which carries or has carried on any trade, business or profession; or any former or existing juristic person, but excludes a public body". A public body means "any department of state or administration in the national or provincial sphere of government or any municipality in the local sphere of government; or any other functionary or institution when exercising a public power or performing a duty in terms of the Constitution or provincial constitution; or exercising a public power or performing a public function in terms of any legislation".

[223] Id 69(2)(a).

[224] Id s 1 defines the term "processing" as "any operation or activity or any set of operations, whether or not by automatic means, concerning personal information, including: (a) The collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use; (b) dissemination by means of transmission, distribution or making available in any other form; or (c) merging, linking, as well as restriction, degradation, erasure or destruction of information".

themselves and that they are informed of what they are consenting to. This consent for processing of personal information must have been done via specified communications, and in a prescribed manner and form.[225] Note should also be had of the fact that the Minister may, in terms of section 69(2) of the POPI Act, issue regulations on the manner and form by which the data subject's consent must be requested.[226]

Section 69(3) requires that the personal information to be processed should be that of the responsible party's customer and that the personal information must have been obtained from the data subject in the context of a sale of products and or services. This provision invokes an opt-in mechanism which requires that a relationship be established before anyone can send unsolicited direct marketing material.[227]

At first glance it appears that the POPI Act has introduced a restrictive measure in regulating spam. For example, by placing an obligation on the responsible person to ensure that before he or she sends the data subject unsolicited communication or direct marketing, he or she must first obtain the consent of the data subject to process his or her personal information.[228]

However, some have raised concerns about these provisions which include:[229]

> that the section is a disappointment in that it still allows a responsible party to approach a data subject at least once to request consent to send direct marketing material if that consent has not previously been withheld. This allowance is strongly opposed due to its scope for abuse, and because, in essence, it reverts back to the opt-out model. In fact, by allowing a responsible party to process personal information once to make the approach to get consent, the prohibition in section 69(1) is reduced to a second-level protection mechanism. That is it becomes relevant after the approach has been made. It is also contrary to the position established in the CPA where a direct marketer must, without exception, assume that a comprehensive pre-emptive block has been registered by a consumer.

The sentiment above has proven to be true in that direct marketers upon hearing that POPI Act was to be enacted in 2013 started approaching potential customers for

[225] Id s 69(1).

[226] Id s 112(2)(f). Also see s 113 on the procedure for making regulation; and Roos 'Data privacy law' 462-3.

[227] Id s 69(3)(a)-(b) read with s 69(1) and (2).

[228] Id s 69(1)(a).

[229] Hamann & Papadopoulos supra n 26; and Papadopoulos supra n 15 238-9.

consent. As a result, there was an increase in unsolicited advances both via e-mail and SMS during that period until today. And as if on cue these direct marketers like Ketler above are quick to point out that the POPI Act allows them to do that at least once. Regarding reverting back to the opt-out mechanism, the POPI Act makes provision for data subjects to "object free of charge" and in a manner free of unnecessary formality to such use at the time of collection.[230] The problematic issue about this is that in most cases the responsible party approaching the data subject for consent would have obtained such personal information from other sources and not from the data subject themselves as the Act provides.[231]

Vermeulen, notes that section 69(1)(a) provides for a soft opt-in mechanism which requires that contact be made once, and that consent be given.[232] Although the issue of consent and a relationship calls for an opt-in mechanism, the POPI Act however, falls short by allowing for an approach to be made once. As noted above in Australia, one cannot send an electronic message seeking consent (for this in itself is considered a commercial message) because it seeks to establish a business relationship.[233] Hence the restrictive approach in prohibiting the sending of unsolicited e-mails without a relationship.[234]

(c) Fraudulent headers or spoofing

The POPI Act addresses and prohibits fraudulent activities such as spoofing or disguising headers.[235] Section 69(4)(a) makes provision for details of the identity of the sender, or the person on whose behalf the communication was sent. This information includes the address or other contact details to which the recipient may send a request that such communication cease.[236] This section aligns with

[230] See s 69(3)(c) of the POPI Act.

[231] Id s 69(3)(a).

[232] See Vermeulen J 'Killing spam softly: POPI in South Africa' http://www.broadband. co.za/ news/telecoms/81759-killing-spam-softly-popi-in-south-africa.html (date of use: 28 January 2016).

[233] See ACMA 'Spam consent' http://www.acma.gov.au/Industry/marketers/Anti-Spam/Ensuring-you-dont-spam/spam-consent-ensuring-you-dont-spam-i-acma (date of use: 15 January 2016)

[234] See the following for contrasting views on the opt-in mechanism: the ITU in Chapter 4 para 4.3.4.2 (c)(ii); Chapter 5 SADC Model Law in para 5.3.4.2 (c)(ii); and Australia's position in Chapter 7 para 7.2.3.2(a) above on the opt-in mechanism.

[235] See s 69(2)(a)(ii) of the POPI Act.

[236] Id s 69(4).

provisions in other jurisdictions such as the USA and Australia above.[237] In fact the POPI Act has picked up where the CPA left off. This provision extends to third parties whom the sender might use in order to send communications for direct marketing. It is hoped that the implementation of this provision will enable the data subject to locate the spammer should he or she wish the solicitation to stop. Hamann and Papadopoulos note that even though a provision is made for falsifying of headers, "section 69(4) does not stipulate what, how or where contact details should be displayed for the purposes of requesting a sender to cease sending further communications".[238]

(d) Harvesting of lists

Section 69(3) of the POPI Act requires that the personal information be processed only if the data subject concerned is a customer of the responsible party, and that his or her information must have been obtained in the course of a sale or service provided, and for the responsible party's similar goods or services.[239] This section covers the issue of the harvesting and sale of lists. This provision should also be read with the following conditions for the processing of personal information – in particular: condition 2 (processing limitation);[240] condition 3 (collection for a specific purpose);[241] condition 6 (openness principle);[242] condition 7 (security safeguards);[243] and condition 8 (data subject participation).[244]

Condition 2 provides for personal information to be processed lawfully and in a reasonable manner that does not infringe on the privacy of the data subject.[245] This information may be processed in an adequate, relevant and not excessive manner.[246] The personal information may only be processed under the following

[237] This issue is covered in para 6.3.2.2 (c) (USA); and para 7.2.3.2 (b) (Australia).

[238] Hamann & Papadopoulos supra n 26 60; and Papadopoulos supra n 15 240.

[239] See s 69(3)(a) and (b) of the POPI Act.

[240] Id s 9-12.

[241] Id s 13.

[242] Id s 17-18

[243] Id s 19-22.

[244] Id s 23-35.

[245] Id s 9(a) and (b).

[246] Id s 10. Roos note that "in terms of this minimality requirement, the amount of personal information collected should be limited to what is necessary to achieve the purpose(s) for which information is processed" (Roos 'Data privacy law' 443).

circumstances: consent for processing is from a data subject or a competent person where the data subject is a child; the processing protects the legitimate interest of the data subject.[247] The data subject must also be given a chance to object at any time to the processing of their personal information for purposes of direct marketing other than direct marketing by means of unsolicited electronic communications in section 69.[248] Section 12 also provides for the collection of personal information to be directly from the data subject with a few exceptions namely: "if the information is contained in or derived from a public record or has deliberately been made public by the data subject; the collection of information from another source would not prejudice a legitimate interest of the data subject". [249]

Condition 3 deals with the purpose-specific condition which requires that personal information be collected for a specific, explicitly defined, and lawful purpose related to the function or activity of the responsible party.[250] Roos note that "the purpose for which such information is collected must be established before any information is collected and that it may not be vague, uncertain or unlawful".[251]

Condition 6 covers the principle of openness, and provides that reasonable practical steps be taken by the responsible party to ensure that the data subject is aware of the following:[252]

> the information being collected and the source from where it was collected in case that information was sourced from a third party; the name and address of the responsible party; the purpose for which the information is collected; whether the supply of such information by the data subject is voluntary or mandatory; any particular law requiring or authorizing the collection of information; and the fact that the responsible party intends to transfer the information to a third party or international organization and the level of protection afforded to the information by that third party or international organization.

This principle avoids the situation where the data is collected in secret and the subject is unaware of who is collecting and for what purposes.[253] It also requires that the responsible party maintain the documentation of all its processing operations.[254]

[247] Id s 11((1)(a) and (d).

[248] Id s 11(3)(b), contrasted with s 69: and Roos 'Data privacy law' 445.

[249] Id s 12(1) and (2). See Roos 'Data privacy law' 443-6 for a discussion of this principle; and Swales supra n 26 61-2.

[250] See s 13(1) and 14 of the POPI Act; Roos 'Data privacy law' 446-7; and Swales supra n 26 62.

[251] Roos 'Data privacy law' 446.

[252] Section 18(1)(a)-((d); (f) and (g) of the POPI Act. Contrast these provisions with s 69(3)(a) of the POPI Act. Also see Roos 'Data privacy law' 449-451.

Condition 7 deals with the security measures on the integrity and confidentiality of personal information. Section 19 puts an obligation on the responsible party to secure the integrity and confidentiality of the personal information in its possession and to take appropriate, reasonable technical and organizational measures[255] to prevent the following: "loss of, damage to or unauthorized destruction of personal information; and unlawful access to or processing of personal information.[256] Those reasonable measures include: identifying all reasonable foreseeable internal and external risks to personal information; establishing and maintaining appropriate safeguards against the risks identified; regularly verify that the safeguards are effectively implemented; and that those safeguards are continually updated in response to new risks or deficiencies".[257] Roos note that appropriate security measures can generally be said to "mean that guarantee a level of security that is appropriate to the risks presented by the processing and the nature of the information to be processed".[258]

Condition 8, the last condition provides for the data subject to be a participant in processing of their personal information, by accessing and correcting such personal information.[259] The right to access will include a request to the responsible person by a data subject to confirm (free of charge) whether the responsible party holds the data subjects personal information; and also a record or description of the personal information in possession of the responsible party.[260] This will also include information about the identity of all third parties or categories thereof that would have had access to the personal information of the data subject.[261] The information requested must be provided within a reasonable time; at a prescribed fee (if any); in a reasonable manner and format; and in a form that is generally understandable.[262]

[253] Id Roos 449.

[254] See s 17 of the POPI Act.

[255] Roos note that: "technical measures will include measures imbedded in the technology used to process the information; and organizational measures will include the use of access codes" (Roos 'Data privacy law' 452).

[256] Section 19(1)(a) and (b) of the POPI Act. Contrast this with reg 4 under the CPA above; Id Roos 451-453; and Papadopoulos and Snail supra n 23 304-305.

[257] Id s 19(2) POPI Act.

[258] Roos 'Data privacy law' 451.

[259] See s 23 and 24 of the POPI Act.

[260] Id s 23(1)(a) and (b; also Roos 'Data privacy law' 453-4; Papadopoulos and Snail supra n 23 305-6; and Swales supra n 26 64-5.

[261] Ibid POPI Act.

[262] Ibid.

The data subject may also request the responsible person to correct or delete personal information in its possession or under its control that is inaccurate, irrelevant, excessive, out of date et cetera.[263] The POPI Act also require that responsible parties ensure that the conditions in chapter 3 of this Act and all the measures that give effect to such conditions are complied with at the time of the determination of the purpose and means of processing and during the processing itself.[264]

The extent to which the POPI Act has gone in safeguarding the processing of personal information is commendable. By so doing, the issue of harvesting and sale of lists had been adequately covered. However, the most important question is what will happen to those lists already in circulation and still being used for marketing purposes once the POPI Act is fully operational. The provisions of the POPI Act will only apply from the time of its promulgation and not retrospectively. Be that as it may, at least data subjects will be in a position to deal with individuals that they have had contact with or whom they have consented to enter into a relationship.

(e) Directories

Section 70(1) of the POPI Act provides that before the subscriber's[265] personal information can be processed, he or she must be aware of the purpose of such collection.[266] The data subject in this instance must be informed free of charge before his or her personal information is processed or included in such directories.[267] This does not apply to editions of directories produced in printed or off-line electronic format before the commencement of this section.[268] Section 70(4) provides "if the personal information of data subjects who are subscribers to fixed or mobile public voice telephony services has been included in a public subscriber directory in

[263] Id s 24(1).

[264] Id s 8 of the POPI Act.

[265] Id s 69(5) of the POPI Act defines the term "subscriber" as "any person who is party to a contract with the provider of the publicly available electronic communications services for the supply of such services".

[266] Id s 70(1)(a) and (b).

[267] Id s 70(1). Section 70(2) further provides that "the objection must be in a manner free of unnecessary formality, to such use of his, her or its personal information or to request verification, confirmation or withdrawal of such information if the data subject has not initially refused such use".

[268] Id s 70(3).

conformity with the conditions for the lawful processing of personal information before the commencement of this section, that information may continue to be included in this public directory in its printed or electronic versions, after having received the information required by subsection (1)".[269]

(f) Enforcement of the POPI Act

Section 39 of the POPI Act establishes a juristic person known as the Information Regulator which will have jurisdiction throughout the Republic.[270] The Information Regulator is an independent institution and is subject to the Constitution and to the law;[271] it must be impartial and perform its functions and exercise its powers without fear, favour, or prejudice,[272] and in accordance with the Act;[273] and be accountable to the National Assembly.[274] The office of the Information Regulator[275] consists of a chairperson[276] and four ordinary members.[277] It must also establish an enforcement committee which must consist of at least one member of the Regulator.[278]

The powers and duties and functions of the Regulator include:[279] to *provide education* by promoting an understanding and acceptance of the conditions for the lawful processing of personal information and the objects of those conditions among others;[280] to monitor and enforce compliance;[281] to consult with interested parties by

[269] Id 70(4); and Roos 'Data privacy law' 461-2.

[270] Id s 39(a); and id Roos 465-471.

[271] Id s 39(b)

[272] Ibid.

[273] Id s 39(c).

[274] Id s 39(d).

[275] See Roos 'Data privacy law' 465-7; also Swales supra n 26 75-7; and Papadopoulos & Snail supra n 23 301 for a discussion of the office of the Regulator.

[276] See s 41(1)(a)(i) of the POPI Act. See the following sections regarding the chairperson: ss 41(1)(c) and (f); 41(2)(a); also s 43 for the duties and powers and functions of the chairperson and other members: ss 41(1)(b), (e), and (g); and s 43 of the POPI Act.

[277] Id s 41(1)(a)(ii).

[278] Id s 50 which deals with the establishment of the enforcement committee.

[279] Id s 40 of the POPI Act. Also Roos 'Data privacy law' 466-7 for a discussion on the tasks of the Information Regulator.

[280] Id s 40(1)(a). Other requirements include: "making public statements regarding any matter affecting the protection of the personal information of a data subject or of any class of data subjects; giving advice to data subjects on the exercise of their rights; and, upon request, providing advice to the Minister or a public or private body on obligations under the provisions and generally on any matter relevant to the operation of the Act" (s 40(1)(a)(ii-v of the POPI Act).

[281] Id s 40(1)(b). The monitoring and enforcing compliance will be by: "public and private bodies with the provisions of the Act; undertaking research into and monitoring developments in

receiving and inviting representations from members of the public on any other matter affecting the personal information of a data subject;[282] to cooperate on a national and international basis with other persons and bodies concerned with the protection of personal information;[283] to handle complaints;[284] to conduct research and report to Parliament;[285] to issue codes of conduct;[286] and to facilitate cross-border cooperation in the enforcement of privacy laws by participating in any initiative aimed at such cooperation.[287] Chapter 10 of the POPI Act deals with enforcement of the Act.[288] Section 73 deals with the interference with the protection of personal information of data subjects in relation with the breach of the conditions for the lawful processing of personal information as prescribed in chapter 3 and also with non-compliance with specific sections of the Act including section 69, 70 and 71.[289] Any person may submit a complaint to the Regulator in the prescribed form and matter alleging interference with the protection of the personal information of a

information processing and computer technology to ensure that any adverse effects of such developments on the protection of personal information of data subjects are minimised and reporting to the Minister the results of such research and monitoring; examining any proposed legislation, including subordinate legislation or proposed policy of the Government that the Regulator considers may affect the protection of personal information of the data subject and reporting to the Minister the results of that examination will be done in the following manner; monitoring the use of unique identifiers of data subjects, and reporting to Parliament from time to time on the results of that monitoring, including any recommendations relating to the need of, or desirability of taking, legislative, administrative or other action to give protection or better protection to the personal information of data subject; and examining any proposed legislation that makes the provision for the collection of personal information by any public or private body" (s 40(1)(b)(i)-(iii); (vii) and (ix)); also Roos 'Data privacy law' 476.

[282] Id s 40(c)(i).

[283] Id s 40(c)(ii).

[284] Id s 40(d). This section includes "the receipt and investigations of complaints about alleged violations of the protection of personal information of data subjects and reporting to complainants in respect of such complaints, gathering such information as in the Regulator's opinion will assist him or her in discharging his or her duties and carrying out his or her functions under the Act; attempting to resolve complaints by means of dispute resolution mechanisms such as mediation and conciliation; and serving any notices in terms of the Act and further promoting the resolution of disputes in accordance with the prescripts of this Act".

[285] Id s 40(e). The research and reporting to Parliament is to be done in the following manner: "from time to time on the desirability of the acceptance by South Africa of any international instrument relating to the protection of personal information of the data subject; and on any matter including necessary legislative amendments relating to protection of personal information that in the Regulator's opinion should be drawn to Parliaments attention".

[286] Id s 40(f). These codes should be: "issued, amended or revoked from time to time; provide guidelines to assist bodies to develop codes of conduct or to apply codes of conduct; and consider afresh, upon application, determinations by adjudicators under approved codes of conduct". See Roos 'Data privacy law' 469-70.

[287] Id s 40(g) read with chapter 9 dealing with transborder information flows; and s 40(h) for general powers and duties exercised by the Regulator.

[288] Id ss 73-99; also Roos 'Data privacy law' 470-5; and Papadopoulos and Snail supra n 23 307-8.

[289] Id s 73(a) and (b).

data subject.[290] Upon receipt of such complaints the Regulator will conduct a pre-investigation;[291] act as conciliator in relation to any interference with the protection of the personal information of a data subject; and conduct a full investigation of the complaint among others.[292]

(g) Penalties

Any person convicted of an offence in terms of the POPI Act will be liable on conviction to a fine or to imprisonment for a period not exceeding ten years, or to both a fine and such imprisonment.[293] Penalties for non-compliance with the provisions of the POPI Act are dealt with under Chapter 11 titled: "Offences, Penalties and Administrative Fines".[294]

8.4.4 Conclusion

The POPI Act was signed into law on 26 November 2013 with the commencement date set for 11 April 2014.[295] Since then the Act has been implemented in phases, and in the view of some commentators, the provisions which have come into operation are not of great significance.[296] Other provisions which will have a huge impact on how spam is regulated in South Africa are dependent on the appointment of the Information Regulator. This much-anticipated event was finally realised with the announcement on 7 September 2016 that the office Information Regulator had been established.[297] This means that the South African landscape regarding the

[290] Id 74 (a).

[291] Id s 79 for pre-investigation proceedings of Regulator.

[292] Id s76 (1).

[293] Id s 107(2); and Roos 'Data privacy law' 475-6.

[294] Chapter 11 deals with a variety of offences, penalties, and administrative fines which include: s 100: obstruction of the Regulator; s 101: breach of confidentiality; s 102: obstruction of execution of warrant; s 103: failure to comply with enforcement or information notices; s 104: offences by witnesses; s 105: unlawful acts by responsible party in connection with an account number; s 106: unlawful acts by third parties in connection with an account number; s 107: penalties; s 108: magistrate court jurisdiction to impose penalties; and s 109: administrative fines. See Roos 'Data privacy law' 475-7.

[295] See Pillay (2014) 14/8 *Without Prejudice* 54.

[296] Ibid; Swales supra n 26 82; and Michaelsons 'POPI commencement date or POPI effective date' http://www.michaelson.co.za/blog/popi-commencement-date-popi-effective-date/13109 (date of use: 28 January 2016). These include: s 1 (definition section); Chapter 5 (Part A Information Regulator); s 112 (regulations); and s 113 (procedure for making regulations).

[297] See Michaelsons 'Information Regulator in South Africa' http://www.michaelsons.co.za/blog/information-regulator-in-south-africa/13893 (date of use: 19 September 2016).

issue of spam will have consequential effects on the existing provisions, especially section 45 of the ECT Act. The next step is for the President to proclaim the commencement of those provisions in the POPI Act which are yet to come into force.[298] The proclamation date will be followed by a grace period of one year from the commencement of a particular section (in this case section 69).[299] The grace period might also be extended by an additional period which may not exceed three years.[300]

The POPI Act does, however, address a number of the concerns identified above, and has aligned itself with other international trends. Issues such as the harvesting of lists and the identification of senders of unsolicited electronic mail are some of the basic requirements included in the POPI Act which are not found in the ECT Act. Some consider the POPI Act's provision on unsolicited communications "a major improvement on section 45 of the ECT Act in so far as it prohibits the processing of personal information for direct marketing purposes unless the data subject has consented (opt-in system) or is – subject to subsection (2) – a customer of a responsible party".[301]

In recent years a number of Bills have also been published which contain anti-spam provisions and these are discussed below.

8.5 Bills on unsolicited electronic communications

8.5.1 ECT Amendment Bill of 2012

8.5.1.1 Introduction

In 2012, a decade after the ECT Act was promulgated, an Amendment Bill was published[302] to, among other things, amend the original Act so as to promote electronic transactions nationally and internationally, and to acknowledge the

[298] Ibid.
[299] See s 114(1) of the POPI Act.
[300] Id s 114(2.
[301] See Papadopoulos supra n 15 240; and Hamann & Papadopoulos supra n 26 59.
[302] Hereafter the 'Amendment Bill'. See supra n 5.

benefits and efficiency of electronic commerce.[303] Although the Amendment Bill proposes a number of amendments to the original Act, focus will only be on amendments proposed to section 45 of the ECT Act, and other related matters.

8.5.1.2 Proposed definition of spam under the Amendment Bill

As indicated above one of the criticisms levelled at the ECT Act was its failure clearly to define what constitutes spam. This proved problematic in the *Ketler* case where the court was forced to turn to the *Oxford Dictionary* to establish what spam is so as to decide whether or not Ketler was a "spammer".[304] The Amendment Bill introduces definitions of what constitutes unsolicited commercial communications, and also other definitions which are important in clarifying the issue of spam. Clause 1 of the Amendment Bill defines "unsolicited communications" as follows:

> Unsolicited communications shall in relation to a data message regarding goods or service, mean that the data message has been transmitted to a consumer by or on behalf of a supplier without the consumer having *expressly* or *implicitly* requesting that data message[305] [emphasis mine].

The Amendment Bill also introduces the terms "commercial communications" and "commercial electronic transaction" which are respectively defined as:

> Commercial communications means a data message sent or received as part of or in anticipation of, a commercial electronic transaction;[306] and
> Commercial electronic transaction[307] means the sale or purchase of goods or services for consideration, whether between businesses, households, individuals, governments, and/or

[303] Other purposes are: "to build confidence in the electronic communications by introducing schemes for the accreditation to authenticate services and products; to help realise the economic and social benefits that can be derived through the use of authenticated services and products in secure global electronic commerce among others" (see cl 1 of the Amendment Bill).

[304] See para 40 *Ketler* case supra n 68. The court defined the noun "spam" as "irrelevant or inappropriate messages sent on the Internet to a large number of newsgroups or users; and, as a verb, the court noted it bears a meaning of sending the same message indiscriminately to (large numbers of newsgroups or users) on the Internet". This definition has to do with volume and not necessarily content.

[305] The term "data message" is defined in the Amendment Bill as "electronic communications including (voice, where the voice is used in an automated transaction; and any form of electronic communications stored as a record". This amendment discards phrases such as: *data generated, sent, received or stored by electronic and includes: the word stored in subsection (b)* of the original term (emphasis mine). See cl 1(q) of the Amendment Bill.

[306] See cl 1(e) of the Amendment Bill.

[307] "Electronic transaction" is defined as "a transaction conducted using electronic communications" (cl 1(v) of the Amendment Bill). This definition puts to rest the concern about the lack of clarity in the original Act as to whether a communication must be classified as electronic format to be spam (Buys supra n 15 161).

> other public or private organisations, that are conducted over electronic communications networks and/or electronic communications facilities, and include the ordering, payment of consideration[308] for and/or delivery of the goods or services in the same way.

The proposed amendment to section 45 provides:

> (1) No person[309] may send unsolicited communications without the permission of the consumer to whom those unsolicited communications are to be sent or are in fact sent.
> (2) No agreement is concluded where a consumer has failed to respond to an unsolicited communication.
> (3) Any person who fails to comply with or contravenes subsection (1) is guilty of an offence and liable, on conviction, to a fine not exceeding R1 million or imprisonment for a period not exceeding 1 year.

8.5.1.3 Commentary on the anti-spam provisions under the Amendment Bill

(a) Background

Clause 45 of the Amendment Bill has three provisions as opposed to the four in the original Act. Section 45(1) of the original Act is amended fundamentally in that it previously legalised spam and thus placed an obligation on recipients to perform certain tasks.[310] The "new" clause 45 makes spam illegal.

The Amendment Bill further clarifies the punishment to be meted out if the provisions of the clause are violated. Clause 45(2) imposes either a fine of one million Rand or one year's imprisonment. The Amendment Bill proposes the deletion of section 45(4) of the original Act (which referred to section 89 of the ECT Act).

(b) Proposed amendments to section 45

Definition(s)

[308] See cl 1(e) of the Amendment Bill which describes the term "consideration" as the meaning given to it in the Consumer Protection Act. Section 1 of Consumer Protection Act, 2008, defines "consideration" as "anything of value given and accepted in exchange for goods or services, including but not limited to: money, property, electronic credit; loyalty credit or award".

[309] According to cl 1(z)(ff) of the ECT Amendment Bill, the term "person" includes "a natural person and any entity recognised as a juristic person and specifically includes a public body". Contrast this with the definition in s 1 of the ECT Act which defines a person as including a public body.

[310] For a general background to the ECT Amendment Bill see Hamann & Papadopoulos supra n 26 60-1; Tladi 'SPAM: An overview' supra n 26 272-4.

The Amendment Bill defines the term unsolicited communications and South Africa will understand spam to be electronic communication transmitted to consumers with the aim of supplying goods and/or services. The commercial aspect is reiterated in the definition of "commercial communications" and "commercial electronic transactions" above, in that the communication should be of an electronic nature and the buying and selling should be undertaken using electronic communications, networks, or facilities.

This definition is consistent with definitions in other anti-spam legislation.[311] The definition of unsolicited communications also invokes the issue of "consent" or "permission".[312] This implies that there must be a relationship between the sender and the consumer before such communications are sent. Terms such as "expressly" and "impliedly" confirm this, despite their not being defined in the Amendment Bill.[313] This definition is in line with the prohibition in clause 45(1) and it invokes the opt-in mechanism, which, as noted above, some have been calling for.

Opt-in mechanism v opt-out mechanism

The opt-in model is consistent with the definition of unsolicited communications above especially where consent is required. This provision lays to rest the criticism that opt-in should be preferred to the opt-out mechanism. However, this notwithstanding, the original section 45(2) is retained and this is somewhat confusing. A restrictive mechanism is introduced which requires that a relationship be established before unsolicited mail is sent to a consumer in terms of section 45(1).[314] However, at the same time the provision still require that the consumer responds to the unsolicited communication by retaining section 45(2) of the original Act. Sense can, however, be made of the section if it is read to imply that an opt-out mechanism should be made available to those individuals who have already opted-in

[311] See: para 6.3.2.1 (USA); and para 7.2.3.1 (Australia) for a discussion on the definitions.

[312] See para 2.14 of the Memorandum on the objects of the Electronic Communications and Transactions Amendment Act, 2012.

[313] See definitions of these terms in Chapter 4 above.

[314] The term "consumer" is defined as "any natural person who enters or intends entering into an electronic transaction with a supplier as the end user of goods or services offered by that supplier, and shall have a meaning given to it in the Consumer Protection Act" (see s 1(f) of the ECT Amendment Bill).

to receive such marketing advances via e-mail, but who, at a later stage, wish to stop receiving such mail. If not, then the Amendment Bill's provision should be read like the POPI Act above, which introduces a soft opt-in to provide for cases where the e-mail is indeed sent and the consumer needs to opt-out.

The fact that a consumer is provided with a new mechanism by which to opt-in, he or she is still obliged to respond to spam e-mails. What remains unclear is whether this provision applies to messages to which the consumer has previously opted-in, or to any other message he or she might receive outside of an extant relationship.

8.5.1.4 Conclusion

From the above it is clear that the proposed provision has at least taken the criticisms levelled against the existing section into account, and has attempted to tighten the grip on spam by introducing the opt-in mechanism. While the Amendment Bill clarifies some of the confusion in the original Act,[315] it still fails to address other practices that exacerbate the problem of spam which include: the harvesting of e-mails; dictionary attacks; falsifying headers; and the use of labels.

Although the amendments were published in 2012, at the time of writing the ECT Amendment Bill is still moot – the anti-spam regime in SA, therefore, remains the opt-out regime. The mere fact that the regime might be transforming from opt-out to opt-in does little to alter the situation. Besides, now that the POPI Act provisions on the issue come into operation, these proposed provisions would not apply as section 45 would be repealed by the POPI Act. Perhaps the reason why there has been so little movement on the ECT Amendment Bill is because of the consideration for POPI Act provisions on spam which will cover more areas than the ECT Act.

8.5.2 Cybercrimes and Cybersecurity Bills of 2015 and 2016

8.5.2.1 Background

[315] See especially the issue of penalties in s 89(1) of the ECT Act.

It is estimated that cyber-related offences are escalating and currently exceed one billion Rand in value annually.[316] As a result, proposed legislation in the form of the Cybercrime and Cybersecurity Bill(s) was published to promote safer communities against cybercrimes and foster security in cyberspace.[317] The Cybercrime Bill highlights the need for South Africa to align with international best practices regarding cybercrimes and cyber security. The Bills were released as follows: the Bill for public comment in 2015 with 30 November 2015 as the deadline for the submission of comments.[318] Only a handful of comments had been received by the due date.[319] In 2016 a follow up Bill was published which took into consideration the comments provided earlier.[320] Note should be taken here that the first cybercrime provisions some of which were highlighted are found in the ECT Act.[321] However, should the Cybercrimes Bill be passed into law some of those provisions in the ECT Act will be repealed.[322]

[316] See South African Government 'Justice publishes draft Cybercrime and Cybersecurity Bill for public comments' (28 August 2015) http://www.gov.za/speeches/justice-publishes-cybercrimes-and-cybersecurity-bill-public-comments-28-aug-2015-0000 (date of use: 28 January 2016).

[317] See Preamble to the Cybercrimes Bill.

[318] Hereafter '2015 Cybercrimes Bill'. See Ellipsis Regulatory Solutions 'The cybercrime and cybersecurity Bill' http://www.elipsis.co.za/cybercrimes-and-cybersecurity-bill (date of use: 28 January 2016).

[319] These comments include: that large portions of the Cybercrimes Bill make sense, however, it is also set to be encroaching upon the constitutional freedoms. See Htxt.africa 'Why the Cybercrimes Bill should concern South Africans' http://www.htxt.co.za/2015/09/14/why-the-draft-cybercrimes-bill-should-concern-south-africans/ (date of use: 28 January 2016) and Ellipsis Regulatory Solutions http://www.elipsis.co.za/cybercrimes-and-cybersecurity-bill. Other comments included: (a) the issue of definitions such as: "critical data", "foreign state", "unlawfully and intentionally access", "law enforcement agency" and "investigator" (see http://www.elipsis.co.za/cybercrimes-and-cybersecurity-bill). Some clauses are set to be broad and vague, in particular: cl 2 (unlawful offence); cl 1 which is set to impose harsher penalties for the dissemination of hate speech online; Ch 6 which covers structures dealing with cybersecurity; and Ch 7 which covers national critical information infrastructure protection. Also see Internet Service Providers' Association 'Draft cybercrimes and cybersecurity Bill 2015' http://www.ispa.org.za (date of use: 28 January 2016)). The problematic issue of stewardship of the Internet being a state security function; and that harsh draconian penalties would muzzle journalists; and that the Bill undermines the POPI Act were also noted as concerns (see, in particular, Right2Know Campaign 'R2K submission on draft cybercrimes and cybersecurity Bill' http://www.r2k.org.za/2015/11/30/cybercrimesbill (date of use: 28 January 2016)).

[320] Hereafter '2016 Cybercrimes Bill'. See supra n 6.

[321] See, in particular, Chapter 13 of the ECT Act which covers the following themes: definitions (s 85); unauthorised access to, intercepting of, or interference with data (s 86); computer related extortion, fraud and forgery (s 87); attempt and aiding and abetting (s 88); and penalties in (s 89). For a discussion on cybercrime provisions in the ECT Act see: Cassim (2011) 44/1 *CILSA* 127-33; also Cassim (2010) 5/3 *Journal of International Commercial Law and Technology* 118-23; Snail (2009) 1 *Journal of Information Law & Technology* 1-13; Van der Merwe 'Criminal Law' 61-78; Gordon 'Internet criminal law' 423-46; and Watney 'Cybercrime and investigation of cybercrime' 336-7 and 347-50; and Collier 'Criminal law and the Internet' 319-47.

[322] See s 61 of the 2016 Cybercrimes Bill for the Schedule of laws to be repealed or amended by the Cybercrimes Bill. The following terms in s 1 will be repealed: "critical data"; "critical

8.5.2.2 Preamble to the Cybercrimes Bill

The preamble to the Cybercrimes Bill makes provision for the creation of offences and the imposition of penalties which have a bearing on cybercrime; to criminalise the distribution of data messages that are harmful and provide interim orders; to further regulation of the jurisdiction for cybercrimes; and to further regulate the powers to investigate, search, access, or seize.[323] It also regulates aspects of mutual assistance in the investigation of cybercrime, and the establishment of a 24/7 point of contact.[324] It would also impose obligations on Electronic Communications Service Providers[325] on aspects which may impact on cybersecurity and repeal and amend certain provisions of certain laws, and connected matters.[326]

8.5.2.3 Anti-spam-related provisions under the Cybercrimes Bills

(a) Background of the Cybercrimes Bills

The Cybercrimes Bills contains a variety of issues relating to cybercrimes and cyber security.[327] However, focus will only be on those provisions related to spam as they appear in both the 2015 and 2016 Bills. Below is a brief outline of these provisions.

(b) Spam-related provisions in the Cybercrimes Bill

database"; and "critical database administrator"; Chapter IX (protection of critical databases) will be deleted; and parts of s 89 (dealing with penalties) will be repealed.

[323] See Preamble to the 2015 Cybercrimes Bill and Cybercrimes Bill 2016.

[324] Ibid.

[325] Hereafter 'ECSP'. Clause 1 of the 2015 Cybercrimes Bill defines the term "ECSP" as: "(a) any person who provides an electronic communications service under and in accordance with an electronic communications service licence issued to such person under Chapter 3 of the Electronic Communications Act of 2005 or who is deemed to be licensed or exempted from being licensed as such in terms of the Electronic Communications Act of 2005; (b) ...; and (c) a person or entity who or which transmits, receives, processes or stores data on behalf of the person contemplated in sub-clause (a) and (b) or the clients of such person; or any other person Also see clause 64 which covers the general obligations of electronic communications service provider liability)". This definition is retained as is in section 1 of the 2016 Cybercrimes Bill.

[326] Ibid.

[327] See the following chapter in the 2016 Cybercrimes Bill: chapter 2 (cybercrimes); chapter 3 (malicious communications); chapter 6 (mutual assistance); and chapter 12 (agreements with foreign states).

The spam related provisions under the two Bills are contained in the part on cybercrimes and include the following: unlawful securing of access; unlawful acquiring of data; unlawful acts in respect of software or hardware tool; unlawful interference with data or computer program; unlawful acquisition, possession … of access codes and passwords. These will be outlined below.

Personal information and financial information related offences

Clause 3 of the 2015 Cybercrimes Bill deals with the prohibition on acquiring; possessing; or providing personal[328] and financial information[329] of another person for purposes of committing an offence.[330] The Bill does not elaborate on what is meant by "committing an offence", but it can be deduced from the provisions that the offence has to do with the cybercrimes contained in the Bill itself. In that case, since spammers need personal information in the form of e-mail addresses or contact numbers, this clause will apply to spam.

The offence extends to anyone found in possession of the personal or financial information of another, if there is a reasonable suspicion that such information was acquired in the manner stated in that clause, and that the person possessing such information is unable to provide satisfactory reasons for such possession.[331] Any person who contravenes the above provisions will be guilty of an offence[332] and will be liable on conviction to a fine not exceeding five or ten million Rand or to imprisonment for a period not exceeding five or ten years, or to both such fine and imprisonment.[333]

Unlawful access

[328] Clause 3(7)(a) of the 2015 Cybercrimes Bill defines the term "personal information" as "any personal information defined under section 1 of the POPI Act". The 2016 Cybercrimes Bill has done away with this provision.

[329] Id cl 3(7)(b) defines the term "financial information" as "any information or data which can be used to facilitate a financial transaction". Also see cl 19 which covers the prohibition of financial transactions. See Cassim (2014) 47 *CILSA* 401 ff for a discussion of phishing and Watney supra n 320 349.

[330] See cl 3(1) and (2) of the 2015 Cybercrimes Bill.

[331] Id cl 3(4).

[332] Id cl s 3(1), (2), (3) and (4).

[333] Id cl 3(2), (5) and (6).

The 2015 Cybercrimes Bill also makes it an offence[334] for anyone to unlawfully and intentionally access[335] or intercept,[336] in whole or in part: data;[337] a computer device; a computer network;[338] a database;[339] a critical database;[340] an electronic communications networks; or a National Critical Information Infrastructure.[341] Any person who contravenes the provisions of sub-clause (1) will be liable on conviction to a fine not exceeding five or ten million Rand or to imprisonment for a period not exceeding five or ten years, or to both.[342] Section 2 of the 2016 Cybercrimes Bill has rephrased the title to read: unlawful securing of access. This section has also

[334] Id cls 4(1) and 5(1).

[335] Id cl 4(3) which defines the term "access" as "to make use of, to gain entry to, to view, display, instruct, or communicate with, to store data in or retrieve data from, to copy, move, add, change, or remove data or otherwise to make use of, configure or reconfigure any resource of a computer device a computer network, a database, a critical database, an electronic communications network or a National Critical Information Infrastructure, whether in whole or in part, including their logical, arithmetical, memory, transmission, data storage, processor, or memory functions, whether by physical, virtual, direct, or indirect means or by electronic, magnetic, audio, optical or any other means". This definition has been modified in the 2016 Cybercrimes Bill.

[336] Id cl 5(3) defines the term "interception of data" as meaning "the acquisition, viewing, capturing or copying of data through the use of hardware or software tool contemplated in section 6(5) or any other means, so as to make some or all of the data available to a person other than the lawful owner or of the data, the sender or the recipient or the intended recipients of the data and includes: examination or inspection of the contents of the data; and diversion of data or any part thereof from its intended destination to any other destination". This term has been left out of the 2016 Cybercrimes Bill.

[337] Id cl 1 Bill defines the term "data" as "any representation of facts, information, concepts, elements, or instructions in a form suitable for communications, interpretation, or processing in a computer device, a computer network, a database, an electronic communications network or their accessories or components or any part thereof and includes a computer program and traffic data". This term has also been modified in s 1 of the 2016 Cybercrimes Bill, and now includes: "electronic representations of information in any form". The term "traffic data" means "data relating to a communication indicating the communications, origin, destination, route, format, time, date, size, duration or type of the underlying service" (this term is retained in the 2016 Cybercrimes Bill); and "data message" means "a data in an intelligible form, in whatever form generated, sent, received, communicated, presented, tendered or stored by electronic means". Section 1 of the 2016 Cybercrimes Bill has retained this term but rearranged it.

[338] Id cl 1 Bill defines the term "computer network" as "two or more inter-connected or related computer devices which allow these inter-connected or related computer devices to: exchange data or any other function with each other; exchange data or any other function with another computer network; or connected to an electronic communications network". This term has been renamed to "computer system".

[339] Id cl 1 defines the term "database" as "a collection of data in a computer data storage medium". This term has been left out from the 2016 Cybercrimes Bill.

[340] Ibid cl 1 defines the term "critical database" as "a computer data storage medium or any part thereof which contains critical data". This term has been left out of the 2016 Cybercrimes Bill.

[341] Id cl 1 defines the term "National Critical Information Infrastructure" as "any data, computer data storage medium, computer device, database, computer network, electronic communications network, electronic communications infrastructure or any part thereof or any building, structure, facility, system or equipment associated therewith or part or portion thereof or incidental thereto". This term has been left out of the 2016 Cybercrimes Bill. Also see s 59 (chapter 11 in the 2016 Cybercrimes Bill) which covers the establishment and control of National Critical Information Infrastructure Fund.

[342] Id cls 4(2)(a-b) and 5(2)(a-b).

replaced the terms above namely: computer program; computer data storage; and computer system.[343]

A person is considered to have secured access to data or a computer program when the person is in a position to: “alter, modify or delete the data; copy or move the data to a different location in the computer data storage medium in which it is held or to any other computer data storage medium; obtain output data; or otherwise use data or computer program; also to cause the computer program to perform any function”.[344] With regards to a computer data storage medium a person would have considered to have secured access if that person is in a position to: “access data as contemplated in s 2(a) or s 2(b) above; stored data or computer program on a computer data storage medium; or otherwise use the computer data storage medium”.[345]

With regards to a computer system a person would be considered to have secured access when that person is in a position to: “use any resources of; instruct; or communicate with a computer system and the access contemplated in s 2(a)-(d) which the person secures is unauthorized”.[346] The term “unauthorized” in this section means “that the person is not himself or herself lawfully entitled to secure access; does not have the lawful consent of another person who is lawfully entitled to secure access; or exceed his or her entitlement or consent to secure access to data, a computer program, a computer data storage medium or computer system”.[347]

Unlawful acquiring of data

Whoever overcomes any protection measure unlawfully or intentionally which is intended to prevent access to data; or acquires[348] data, within or which is transmitted to or from a computer system is guilty of an offence.[349] The same applies to the

[343] See s 2(1) of the 2016 Cybercrimes Bill.

[344] Id s 2(2)(a) and (b).

[345] Id s 2(c).

[346] Id s 2(d).

[347] Id s 2(3).

[348] The term “acquire” means “to use; examine or capture data or any output thereof; copy data; move data to a different location in a computer system in which it is held or any other location; or divert data from its intended destination to any other destination”. Id s 3(4).

[349] Id s 3(1).

possession of data with the knowledge that a person will be guilty if such data was acquired unlawfully in terms of s 3(1).[350] Any person found in possession of data, in regard of which there is a reasonable suspicion that such data was acquired unlawfully as contemplated in s 3(1) and that person is unable to give satisfactory account of such possession is also guilty.[351]

Unlawful acts in respect of software or hardware tool

Clause 6 of the 2015 Cybercrimes Bill covers unlawful acts in respect of software and or hardware tools.[352] This clause makes it an offence "for any person who unlawfully and intentionally manufactures, assembles, obtains, sells, purchases, makes available, or advertises any software or hardware tools for the purpose of contravening the provisions in clauses 3(1)(a); 4(1) or 5(1)".[353] Clause 6 also extends to the use and possession of any software or hardware tool in contravention of the clauses above.[354] Any person found in possession of software or of hardware tools where there is a reasonable suspicion that the items are held for the purpose of contravening the provisions above, and who is unable to provide satisfactory reasons of such possession, will be guilty of an offence.[355] A person contravening sub-clauses (1), (2) or (3) will be liable to a fine not exceeding five million Rand or to imprisonment for a period not exceeding five years, or to both such fine and

[350] Id s 3(2).

[351] Id s 3(3).

[352] Id cl 5. Also see s 4 of the 2016 Cybercrimes Bill. The term "software or hardware tools" is defined in cl 5(5) as "any data, electronic, mechanical or other instrument, device, equipment, or apparatus, which is used or can be used, whether by itself or in combination with any other data, instrument, device, equipment or apparatus, in order to: acquire, make available or to provide personal information or financial information as contemplated in particular clauses; access as contemplated in clauses 4(3); intercept data as contemplated in s 7(3); interfere with data as contemplated in cl 7(3)". This term has been expanded in s 4(3) of the 2016 Cybercrimes Bill to also include "acquiring, modifying, providing, making available, copying, using or cloning a password, access code or similar data or devices as defined in s 7(3)". The term "computer program" means "a sequence of instructions which enables a computer device to perform specified functions" (see s 1 of the 2016 Cybercrimes Bill).

[353] Clause 6(1) of the 2015 Cybercrimes Bill; also id s 4(1). Obviously the clauses mentioned therein are replaced by the following provisions in the 2016 Cybercrimes Bill: s 2(1) deals with securing access unlawfully); s 3(1) covers the issue of unlawfully acquiring of data; s 5(1) this covers the issue of unlawfully interfering with data or computer program; s 6(1) unlawful interference with computer data storage medium or computer system; or 7(1) (a) and (d) unlawful acquisition, possession, provision, receipt, or use of password, access codes or similar data device.

[354] Id cl 6(2).

[355] Id cl 6(3); also s 4(3) of the 2016 Cybercrimes Bill.

imprisonment; or to a fine not exceeding ten million Rand or to imprisonment for a period not exceeding ten years, or both such fine and imprisonment.[356]

Unlawful interference with data; computer program; computer data storage medium and computer system

Section 5 makes it an offence for anyone who unlawfully and intentionally interferes with data; or computer program.[357] The same applies with regard to computer data storage medium or computer system.[358] The phrase "interference with data or computer program" means "to permanently or temporarily:[359] delete or alter data or a computer program; render vulnerable, damage or deteriorate data or a computer program; obstruct, interrupt or interfere with the lawful use of data or computer program; and deny access to data or a computer program".

Unlawful acts in respect of malware

Clause 9 covers the unlawful acts in respect of malware, and makes it an offence for any person to assemble, obtain, sell, purchase, possesses, make available, advertise, or use malware[360] for the purposes of unlawfully and intentionally causing damage to data et cetera.[361] Any person who is found in possession of malware and there is a reasonable suspicion that it is held for purposes of unlawfully and internationally causing damage to data, a computer device, et cetera, and who is unable to give a satisfactory account of his or her possession is likewise guilty of an offence.[362] Any person who contravenes the provisions of sub-clauses 1 and 2 is liable to a fine not exceeding five million Rand or to imprisonment for a period not

[356] Id cl 6(4). The 2016 Cybercrimes Bill provides for penalties in s 14 (2) which are the same as the 2015 Cybercrimes Bill.

[357] See s 5(1) of the 2016 Cybercrimes Bill.

[358] Id s 5(1).

[359] Id s 5(2).

[360] Id cl 9. The term "malware" is defined in cl 9(4) as "any data, electronic, mechanical or other instrument, device, equipment, or apparatus that is designed specifically to: create a vulnerability in respect of; modify or impair; compromise the confidentiality, integrity or availability; or interfere with the ordinary functioning or usage of, data, a computer device, a computer network, a database, a critical database, an electronic communications networks, or a National Critical Information Infrastructure".

[361] Id cl 9(1). The clause includes damage caused on the following: a computer device, a computer network, a database, a critical database, an electronic communications network, or a National Critical Information Infrastructure.

[362] Id cl 9(2).

exceeding five years, or to both a fine and imprisonment.[363] It is important to note here that the 2016 Cybercrimes Bill has done away with this clause.

Unlawful acquisition, possession, provision, receipt or use of password, access codes or similar data or devices

Section 7 of the 2016 Cybercrimes Bill makes it an offence for any person who unlawfully and intentionally acquires, possesses, provides to another person, or uses a password, an access code or similar data device for purposes of contravening the provisions in this Bill.[364] If there is reasonable suspicion that anyone has acquired, or is in possession … of passwords or access codes for purposes of contravening provisions of this Bill and those persons are unable to give a satisfactory account of such possession, then they will be guilty of an offence.[365] The terms "password, access codes" or "similar data device" are defined as:[366]

> a secret code or pin; an image; a security token; an access card; any device; biometric data; or a word or a string of characters or numbers used for financial transactions or user authentification in order to access data, a computer program, a computer data storage medium or a computer system.

This provision is in line with the international trends as noted in Chapters 6 and 7 – ie, harvesting and especially the use of dictionary attacks.[367] The following terms are indicative of such practices: *using software* to *obtain*, *sell*, *purchase*, *acquiring*, *interfering*, *cloning a password or codes*, make available or *advertise e-mail addresses*. All these are deceptive practices that spammers use to acquire personal information of recipients in order to send spam. Any person who unlawfully and intentionally attempts; conspires with any other person; aids, abets, induces, incites, instigates, instructs, commands or procures another person to commit an offence in terms of the above provisions is guilty of an offence and will be liable on conviction to the punishment to which a person convicted of actually committing that offence

[363] Id cl 9(3).

[364] See s 7 (1) of the 2016 Cybercrimes Bill. The affected provisions include: ss 2(1); 3(1); 5(1); 6(1); 8 or 9 of the 2016 Cybercrimes Bill. This section reads the same as cl 10 of the 2015 Cybercrimes Bill.

[365] Id s 7(2), contrast with cl 10(2) of the 2015 Cybercrimes Bill.

[366] See 7(3)(a) and (g) of the 2016 Cybercrimes Bill; also cl 10(4) of the 2015 Cybercrimes Bill.

[367] See para 4.3.4.2 (c) (iv); para 6.3.2.3 (c); and para 7.2.3.2 (d).

would be liable.[368] Clauses 3-5 and 9 above will be considered as aggravating factors if the offence was committed in concert with one or more persons.[369]

(c) Enforcement

Clause 64 addresses enforcement issues and also addresses the general obligations of the ECSP. It provides for reasonable steps to be taken in order to inform the clients of cybercrime trends which affect or may affect them.[370] The clause also sets out procedures by which service providers' clients can report cybercrimes to the ECSP. The ECSP is obliged to inform its clients of measures they may take in order to safeguard themselves against cybercrime.[371]

An ECSP that is aware, or becomes aware, that its computer network or electronic communications network is being used to commit an offence provided in the Bill, must immediately report the matter to the National Cybercrime Centre and preserve any information which may assist law enforcement agencies in investigating the offences.[372] This includes information which reveals the origin, destination, route, time, date, size, duration, and type of the underlying services.[373] The ECSP which fails to comply with the sub-clauses above is guilty of an offence and liable on conviction to a fine of ten thousand Rand for each day on which such failure to comply continues.[374]

8.5.2.4 Commentary and conclusion

The Cybercrimes Bills are another addition to the country's ever-evolving anti-spam arsenal which promises to close the gaps, especially where computer-related crimes and activities are involved. The 2015 Bill specifically addresses the technical aspects of spam such as the use of malware,[375] financial information (phishing),[376] and

[368] Id s 12 of the 2016 Cybercrimes Bill, contrast with cl 22 of the 2015 Cybercrimes Bill.
[369] See cl 23 of the 2015 Cybercrimes Bill; also s 11(1) and (2) of the 2016 Cybercrimes Bill.
[370] See cl 64(1) of the 2015 Cybercrimes Bill; also s 20 of the 2016 Cybercrimes Bill.
[371] Ibid 2015 Cybercrimes Bill.
[372] Id cl 64(2)(a).
[373] Id cl 64(2) (b).
[374] Id cl 64(3).
[375] Id cl 9.
[376] Id cl 19.

software and hardware tools used to gain access to such information.[377] The Cybercrimes Bill proposes the criminalisation of such acts and the penalties for such offences are clearly set out. The Bill applies to offences and acts or omissions committed in the Republic, and “a court in the Republic” will try those offences.[378]

The global nature of cybercrimes presents challenges for South Africa and other nations wishing to address this issue. Some have noted that: “domestic solutions are inadequate in cyberspace because there are no geographical or political boundaries, and many computer systems can be easily accessed from anywhere in the world so rendering domestic laws increasingly obsolete”.[379] The Cybercrimes Bills have addressed this concern in clause 65 which provides for agreements to be entered into with foreign states for mutual assistance and cooperation with regards to investigations into and prosecution of offences relating to cybercrime.[380] This aligns with the provisions in the POPI Act.[381] Cassim has advanced the following solutions as a way forward for SA in addressing cybercrime:[382]

> Encouraging Internet users to share the burden of securing information privacy where feasible; education in computer ethics should also be taught in schools to educate learners about the negative consequences of committing cybercrime; and this should be expanded to continuous research and training of IT security personnel, finance service sector personnel, police officers, prosecutors, and the judiciary to ensure that they remain abreast of the ever-changing computer technology.

The 2016 Cybercrimes Bill has still not been promulgated, but should it become law its beneficial effect will lie in its technical measures – particularly as regards the use of software for harvesting lists.

[377] Id cl 6.

[378] Id cl 25(1). The Bill fails to note the court.

[379] See Cassim (2010) supra n 321 123 and Cassim (2011) supra n 321 137.

[380] See Ch 10 of the 2015 Cybercrimes Bill.

[381] See chapter 9 of POPI Act dealing with trans-border information flows; also ch 6 of the 2016 Cybercrimes Bill; and Chs 6 and 7 on international initiatives by the USA and Australia in combating spam.

[382] See Cassim (2011) supra n 321 123.

8.6 Contextualisation of South Africa’s anti-spam and direct-marketing provisions

8.6.1 Introduction

In outlining South Africa’s anti-spam provisions, it has become clear that these are scattered throughout a number of pieces of legislation noted which address a variety of issues. These legislative pieces have spanned a decade and continues to this day. The creation of an industry body to deal with these spam matters and related issues, and the interpretation of the relevant provisions by a court of law, have added value to the discourse, but a solution to the problems identified remains elusive. What the legislative pieces have done is to create a fragmented system which complicates issues considering that spam is also a global problem. This exposes South African consumers to rouge marketers within its borders, and also a possible safe haven for spammers as was noted in Chapter 5 above. Until this system is rectified, the problem will escalate with no solution in sight. An outline of how the fragmented system looks and how to work towards its alignment with international best practices is offered in what follows.

8.6.2 Overlapping laws

The laws outlined above often overlap; and in some instances they complement each other. Where overlaps or intersections occur, provision is made in those laws on how to deal with the overlaps. Obviously, these laws each define the issue of spam differently, each contains different mechanisms, and the penalties prescribed in the legislation also differ.

8.6.2.1 ECT Act and the CPA

The ECT Act makes provision for consumer rights within an online environment, whereas the CPA applies mainly in an offline environment. The provisions of the two Acts must be read and applied together. In terms of the CPA, where the legislation conflicts and concurrent application is not possible, the provision that extends the greater protection to consumers prevails over an alternative provision.[383] The coming into operation of the CPA has also amended certain provisions in the ECT Act, especially those that relate to the Consumer Affairs Committee which has been replaced by the National Consumer Commission.[384] In coming to its decision, the court in the *Ketler* case also noted that the CPA and the ECT Act will run concurrently, especially with regard to the issue of self-regulation.[385]

8.6.2.2 ECT Act, CPA and the POPI Act

The first step toward consolidation of laws was taken when the POPI Act was signed into law in 2013. The anti-spam provisions apply only to electronic direct marketing, under the POPI Act and the CPA to non-electronic marketing. Where both provisions of the Acts apply and provisions are in conflict, section 2(9) of the CPA will determine which law takes precedence.[386]

The coming into operation of the POPI Act has had the effect of repealing sections 45, 50 and 51 of the ECT Act.[387] The term "personal information" in section 1 of the ECT Act is to be replaced by that in the POPI Act. As noted above, the POPI Act is being implemented in phases, and the first phase covering the definition section is now in operation. The second phase of implementation will unfold only after the appointment of the Information Regulator – a process which only took place in September 2016.

The coming into operation of the next phase means that the POPI Act will make the sending of spam illegal if the responsible person sends such without the consent of the recipient. However, sections 11 and 12 of the CPA will run concurrently with section 69 of the POPI Act when dealing with the issue of spam.

8.6.3 Harmonisation of laws

[383] See s 2(9)(b) of the CPA.

[384] Id Schedule 1(B); and Naude & Eiselen supra n 106 121.3.

[385] See para 81 of the *Ketler* case supra n 68; and Pistorius & Tladi supra n 26 703-4 for a discussion on overlapping of laws.

[386] See De Stadler supra n 15 62.

[387] See Schedule 1 of the POPI Act.

8.6.3.1 Introduction

As mentioned at the outset, the purpose with this chapter was not only to highlight legislative measures regulating spam, but also to question whether it is viable to have a number of anti-spam and direct-marketing provisions dealing with a single issue but prescribing contradictory requirements. Some are of the view that “spam and direct marketing online have not been viewed in a holistic context, and that this has resulted in the fragmented approach found in the legislations above”.[388] Although South Africa appears to have most provisions that can make for an anti-spam law in place, the downside is that the system is fragmented.

8.6.3.2 Requirements for sending electronic communications

(a) Defining the problem

Almost all the Acts that are discussed above define the terms for sending electronic communications satisfactorily. Some include additional concepts which better outline and enhance the scope of the problem. For example, the following definitions are covered in these laws: advertising or advertisement;[389] commercial communications; commercial electronic transactions;[390] consumer;[391] data subject;[392] direct marketing;[393] electronic communications;[394] person;[395] personal information;[396] and unsolicited commercial communications.[397]

Hamann and Papadopoulos note:[398]

> the definitional variations between the ECT Act, the CPA and the PPI[399] should be carefully considered and harmonised as far as possible. …direct marketing online may not limit its

[388] See Hamann & Papdopoulus supra n 26 61; Papadopoulos supra n 15 240.

[389] See s 1 of the NCA and the CPA.

[390] See cl 1(e) of the ECT Amendment Bill.

[391] See s 1 of the ECT Act, the NCA, and the CPA.

[392] Ibid the ECT Act and POPI Act.

[393] See s 1 of CPA and the POPI Act.

[394] Contrast s 1 of the ECT, CPA, and POPI Act.

[395] See s 1 of the CPA; s 1 of the POPI Act; and s 1 of the ECT Act.

[396] See s 1 of the POPI Act which has substituted s 1 of the ECT Act.

[397] See s 1(ss) of the ECT Amendment Bill. This definition is consistent with the direct marketing definitions under the CPA and the POPI Act.

[398] Papadopoulos supra n 15 239; and Hamann & Papadopoulos supra n 26 59-60.

[399] Others refer to the Protection of Personal Information Act as the PPI.

> activities to the sending of text, sound, voice and image. It should also include collecting data through software and cookies which are data files.

The above authors further note:[400]

> in trying to enforce a regulatory framework in an online environment, the enforcer must consider the different fields of application for each Act, and that the different definitions for terms like electronic communications and, more importantly, the overlapping and at times conflicting web of legislative provisions applicable to direct marketing or unsolicited commercial electronic communications, need to be included in the Act.

(b) Opt-in v opt-out mechanism

As noted above, the South African regime still applies the opt-out mechanism which is encountered in various Acts.[401] The CPA has taken a step in the right direction by making provision for a pre-emptive block[402] which will enable consumers to register to opt-out of unwanted direct marketing e-mails. The CPA; NCA and the POPI Act provides that the opt-out mechanism must function free of charge,[403] and that consumers may not be contacted at home for direct marketing purposes unless prior arrangements have been made.[404] With the establishment of the office of the Information Regulator the opt-out mechanism will be replaced by an opt-in mechanism.

(c) Harvesting and sale of lists

Since personal information can be obtained in a variety of ways, there is a need to provide for the issues of harvesting and the sale of lists. The CPA prohibits the administrator from providing, selling, or otherwise disposing of any information contemplated in Reg. 4 of the CPA, to anyone, unless the express, written permission of the consumer has been obtained.[405] The NCA also covers this issue by allowing consumers to opt-out of marketing or customer lists that might be sold or

[400] Papadopoulos supra n 15 239.

[401] See s 45(1) of the ECT Act; s 11(2) of the CPA; s 74 (6)(a) of the NCA; and s 69(4)(b) of the POPI Act.

[402] See s 11(1)(c), (3) and (4) read with reg 4(3) of the CPA; and s 74(7) of the NCA.

[403] Id s 11(5); and s 69(3)(c) of the POPI Act.

[404] Id s 12; and s 75(2) of the NCA.

[405] See reg 4(e) of the CPA; contrast this with s 12; of POPI Act; and s 7 of the 2016 Cybercrimes Bill.

distributed by credit providers[406] in contravention of the Act.[407] This also includes the distribution of e-mail or SMS messages.[408] The POPI Act, on the other hand, requires that only personal information of a data subject who is the customer and whose contact details were obtained in the context of the sale of a product or service may be processed.[409] This also applies in instances where electronic directories are compiled – the data subject must be informed before such information is included in the directory.[410] The POPI Act also elaborates on this issue by providing conditions for lawful processing of personal information as outlined above. Even the Cybercrimes Bill(s) makes provision for unlawful acts in respect of software and hardware tools which make obtaining, selling, or purchasing any software tools an offence.[411] If enacted, the Cybercrimes Bill will add value to the regulation of the use of software for purposes of extracting the personal information of recipients in order to send spam e-mails.

(d) False headers and spoofing

Falsifying headers is provided for in section 69(5) of the POPI Act which requires that "any communication for the purpose of direct marketing, should contain details of the identity of the sender or the person on whose behalf the communication has been sent, together with an address or other contact details to which the recipient may send a request that such communications cease".[412] This section also applies to third parties who might be acting on behalf of the sender. Some have noted that while this issue has been addressed, "it is, however, inadequate as the Act fails to provide how and where those contact details need to be displayed".[413]

(e) Labelling

[406] The term "credit provider" in respect of a credit agreement to which this NCA applies means among others: "the party who supplies goods and services under a discount transaction, incidental credit agreement or instalment agreement; the party who advances money or credit under a pawn transaction; and a party who extends credit under a credit facility". See s 1 of the NCA for an exhaustive list.

[407] Id s 74(6)(b)(ii).

[408] Id s 74(6)(b)(iii).

[409] See s 69(3) of the POPI Act.

[410] Id s 70(1) and (2).

[411] See s 6 of the 2016 Cybercrimes Bill.

[412] See s 69(4) of the POPI Act.

[413] See Hamann & Papadopoulos supra n 26 60.

The only legislation that contains labelling provisions is the NCA which requires that certain marketing information disseminated on behalf of a credit provider include a statement with the prescribed information for that particular solicitation.[414] As noted above, labelling is important when it comes to the content of the message. Perhaps the POPI Act, as the default provision on spam, should be amended to include the labelling requirement. In that case recipients will be in a position to know the contents of the message before they open it and be able to make an informed decision before exposing themselves to messages with inappropriate content. The POPI Act should also specify where the label is to be placed and also to provide for the consequences for not adhering to that. In this case lessons from the USA and Australia above will be of value.

(f) Enforcement and penalties

The nature of enforcement depends on the Act concerned. The following institutions currently enforce the provisions of the various laws: the National Consumer Commission; the National Credit Tribunal; and the Information Regulator.[415] The penalties also differ in that some of the legislation regard spam or spam-related activities as crimes punishable by imprisonment, a fine, or both. The periods of imprisonment differ as do the extent of the fines.

8.7 Conclusion

South Africa has come a long way in attempting to redress some apartheid laws by adopting consumer-oriented laws to protect its consumers. This indicates that South Africa is doing its part to align with international best practices. While these measures are admirable, their weakness lies in the fragmented system in which they are found. In addressing the loopholes in the regulation of spam, commentators have suggested that: “the legislature drafts a comprehensive, holistic and comparative overview of current trends in legislative interventions, and that a concerted effort be made to harmonise the POPI Act, and CPA taking into consideration criticisms

[414] See s 77 of the NCA.

[415] See the discussion on these institutions: NCC in para 8.3.4.5; Information Regulator para 8.4.3 (f); ECSP para 8.5.2.3 (c); including the industry regulators: DMASA in para 8.3.4.4 (c); and ISPA 8.2.6.2 above.

above".[416] In addition "the signing of the POPI Act into law with the inception of the eight conditions for data processing will at least clarify the situation".[417] The coming into operation of section 69 of the POPI Act will repeal the problematic sections 45, 50, and 51 of the ECT Act and other related matters. Taking into consideration the fact that the (soft) opt-in mechanism in the POPI Act is still another way of soliciting business from consumers then an amendment of the current provisions should be considered to include the suggestions outlined above in order to provide adequate protection. Most of the requirements for the dissemination of unsolicited electronic communications are already in place in the pieces of legislation identified above. These can be consolidated into a single document to regulate spam.

South Africa should also acknowledge that spam is an international problem respecting no borders, affecting a variety of stakeholders, and as such it needs to act globally by partnering with other nations so as to keep each other abreast of the challenges posed by spam. The POPI Act with its trans-border provisions will in this case be a valuable contribution in that aspect although only focusing on data protection. As such South Africa would "think locally and act globally" as noted by the ITU above.

In the final chapter of this thesis a multi-faceted approach to the ever-increasing problem of spam in South Africa is outlined.

[416] See Papadopoulos supra 15 240; Hamann and Papadopoulos supra n 26 61.
[417] See Swales supra n 26 70.

CHAPTER 9

RECOMMENDATIONS AND CONCLUSION

9.1 Summing up the issues

The thesis started by asking whether South Africa's current minimalistic and overlapping anti-spam and direct marketing provisions are adequate to protect consumers. It also sought to determine whether introducing more restrictive legislation will better protect online consumers from receiving spam. Lastly, it sought to establish whether a Model Law would be an appropriate starting point in aligning South Africa's legislation with international best practices aimed at combating spam.

In addressing these questions an analysis of what has been done to combat spam internationally, regionally, and in foreign jurisdictions was conducted. It was highlighted that the South African spam regime is fragmented, and a point was made that when the POPI Act comes fully into operation, it will limit spam to only where an approach is a (soft) opt-in. It was concluded that even if South Africa were to introduce a (soft) opt-in regime – a move long called for – section 69 of the POPI Act read with the conditions for lawful processing would still lack certain important requirements for the dissemination of commercial e-mail found in the anti-spam laws discussed above.

Therefore, in order for South Africa to align itself properly with international best practices, a multi-faceted approach in combating spam is highly recommended. This approach will first deal with spam at a local level and also adopt measures to deal with the influx of spam from beyond its borders.

9.2 A multi-faceted approach to combating spam

A multi-faceted approach has been recommended by the ITU and the OECD above and is also part of Australia's strategy in combating spam. Should South Africa take this route, this approach will not only be in line with other jurisdictions, but will also be a solution that has been called for by other commentators in the region. The multi-faceted approach will therefore include the following: strong legislation;

consumer education; technical measures; industry partnerships; and international cooperation.

9.2.1 Strong legislation

As a first step toward combating spam, it is strongly recommended that South Africa enact a specific anti-spam law at national level. Lessons on the drafting of such an Act can be drawn from other anti-spam laws, model laws, and instruments discussed above. The Model Law will therefore include the following:

9.2.1.1 Definition section

The following definitions, some of which already feature in South African anti-spam provisions above, must be included in the definition section: advertising/advertisement;[1] commercial electronic message; commercial communications;[2] commercial e-mail message;[3] commercial electronic transaction;[4] consent[5] (including the following types of consent: affirmative consent;[6] assumed consent;[7] express consent;[8] and inferred consent);[9] consumer; dictionary attacks; direct marketing;[10] donation; electronic transactions;[11] e-mail address;[12] e-mail message;[13] false and misleading;[14] harvested address list;[15] header information;[16] Internet domain name;[17] recipient; sender; spoofing; and unsolicited communications

[1] As defined in s 1 of the CPA; also s1 of the POPI Act.

[2] See s (6)(1)(a-c) of the Spam Act of 2003; also s 1(e) of the Amendment Bill.

[3] See s 3(2)(A) of the CAN-SPAM Act.

[4] See s 1(e) of the Amendment Bill.

[5] See s 4 of the Spam Act.

[6] Section 3(1)(A) and (B) of the CAN-SPAM Act; also s 1 POPI Act.

[7] See OECD Anti-spam Toolkit 9 and 27-28 http://www.oecd.org/internet/consumer/36494147.pdf (date of use: 21 March 2016).

[8] ACMA 'Spam consent' http://www.acma.gov.au/Industry/marketers/Anti-Spam/Ensuring-you-dont-spam/spam-consent-ensuring-you-dont-spam-i-acma (date of use: 21 March 2016).

[9] Ibid.

[10] As defined in s 1 of CPA and POPI Act.

[11] See s 1(v) of the Amendment Bill.

[12] See s 3(5) of the CAN-SPAM Act.

[13] See s 3(6) of the CAN-SPAM Act.

[14] When used in relation to commercial e-mail: see s 16-9-100 (10) (A)-(G) of the Official Code of Georgia; also s 1497 (5) Maine Statutes.

[15] See s 4 of the Spam Act.

[16] See s 3-805.1(6) of the Maryland Criminal Code; also s 2913.421 (A) (7) of the Ohio Revised Code.

[17] See s 407.1120 (6) of the Missouri Revised Statutes; also s 37-24-36(6) of the South Dakota Codified Laws; and s 46.001(9) of the Texas Statutes.

in all its variations as noted in the previous chapters.[18] The legislation should strive to include all relevant terms for clarity and ease of reference. These definitions should also allow for future technological developments.

9.2.1.2 Rules for sending electronic communications

The rules of sending unsolicited electronic mail should be extensive as possible and most importantly take the protection of consumers into consideration. The following rules should therefore be included in the anti-spam law:

(a) Prohibition for the sending of commercial e-mail (opt-in mechanism)

The Model law should prohibit spam in all its forms and not make an allowance for an approach before a relationship. The provision should read as follows: "A person must not send, or cause an unsolicited electronic message to be sent, for purposes of marketing his or her goods or services unless consent has been given prior to such an approach".[19] In addition to this, an unsolicited electronic message may only be sent where an opt-in requirement has been met.[20]

(b) Provision to opt-out of unwanted commercial e-mail

The Model law should also provide for an opt-out mechanism in cases where consumers would no longer want to receive the unsolicited messages. Here the provisions of the SADC Model Law on marketing by means of electronic communication should be applied.[21] The sender should also provide the recipient with a functioning return e-mail address(s) which the recipient can use to submit, or as a reply to an e-mail message or other form of Internet-based communication, requesting not to receive future commercial e-mail messages from the sender at the e-mail address where the message was received.[22] The opt-out facility should be able to receive such messages or communications for no less than (a specified

[18] See in particular chapter 6 and 7 above.

[19] See s 18(1) of the Spam Act.

[20] See s 30(2) of the SADC Model law.

[21] Section 30 of the SADC Model law provides the recipient with a valid and operational opt-out facility or other Internet-based mechanism, clearly and conspicuously.

[22] See s 5(a)(5)(ii) of the CAN-SPAM Act.

amount of days) after the transmission of the original message.[23] The sender who fails to provide the recipient with an operational opt-out facility, will be guilty of an offence and liable, on conviction.[24] An opt-out facility should further reflect the sender's identity and contact details, including its place of business, e-mail addresses, and telefax numbers; and the identifying particulars of the source from which the sender obtained the recipient's personal information.[25] A sender would not be liable if a return e-mail address or other mechanism is unexpectedly and temporarily unable to receive messages or process requests due to technical problems beyond the control of the sender, with the provision that the problem is rectified within a reasonable period.[26]

The opt-out mechanism should be able to be processed free of charge as contained in the POPI Act and CPA provisions. The regulatory body in that regard must also be aligned so that those consumers who receive unwanted SMS messages should not be penalised to opt-out of such messages.

(c) Prohibition on falsifying or misleading header and information

The Model Law should prohibit the transmission of unsolicited electronic messages that: contains false, deceptive, or misleading information in its subject line; uses a third party's Internet domain name without the permission of that third party; or otherwise fraudulently misrepresents or obscures any information in identifying the point of origin or the transmission path of the unsolicited electronic messages.[27] In addition to the POPI Act's provision on identifying the sender or the person on whose behalf the communication has been sent,[28] the Model Law should also include that: a person who intentionally sends, or cause an unsolicited electronic message to be sent, must make sure that the message clearly and accurately identifies the individual or organisation which authorised the sending of the message.[29] It should

[23] Id s 5(a)(3)(A)(i-ii).

[24] See s 30(5) of the SADC Model law; also s 5(a)(5)(iii) of the CAN-SPAM Act.

[25] Id s 30(1)(a) (b) of the SADC Model Law.

[26] See s 5(a)(3)(C) of the CAN-SPAM Act.

[27] See s 6-47-2 (d) of the Rhode Island General Laws: Title 6 Commercial Law General Regulatory Provisions; Chapter 47 Internet Access and Advertising by Facsimile (added in 1999).

[28] See s 69(4)(c) of POPI Act.

[29] See s 17(1) of Spam Act.

also make it unlawful for any person to initiate the transmission of an unsolicited electronic messages containing, or is accompanied by, header information that is materially false or materially misleading.[30] The message should include accurate information on how the recipient can readily contact that individual or organisation; a declaration that the information complies with the condition(s) (if any) specified in the regulations; and an undertaking that information is reasonably likely to be valid for at least thirty days after the message has been sent.[31]

The information should form part of the header information of the message. This section will not apply if the sender was unaware, or could not, with reasonable diligence, have ascertained, that the message was sent or caused to be sent; and if the person sent the message, or caused the message to be sent by mistake.[32]

(d) Labelling of commercial e-mail messages

The Model law should also have provisions on labelling of messages. It should make it unlawful for any person to initiate the transmission of an unsolicited commercial electronic message unless the message provides clear and conspicuous identification that it is an advertisement or a solicitation.[33] An unsolicited electronic message should include in its subject line "ADV" (advertisement) as the first characters;[34] and if the message contains explicit sexually material that may only be viewed or purchased by individuals over the age of eighteen years, the subject line of each message must include "ADV: ADLT" as its first characters in the subject line.[35] This should also include electronic communications with a political content.

(e) Prohibition on harvesting and sale of e-mail addresses

[30] See s 5(a)(2) of CAN-SPAM Act.

[31] Ibid.

[32] See s 17(2)(a) and (b); and 17(3) of the Spam Act.

[33] See s 5(a)(5)(i) of the CAN-SPAM Act.

[34] See s 52-570c. (b) of the General Statutes of Connecticut; also section 668.603. (1)(c) and (d) of the Florida Statutes.

[35] See s 50-6-107 (c) (1) (E) of the Kansas Statutes; also section 51.1741.1 (5) Louisiana Revised Statutes Title 51; section 1497 (3) (2) of Maine Statutes.

The CPA and the POPI Act have made provision for harvesting and selling of lists. However the Model law should be specific as to what it is prohibited, for example: it should also include the following terms in its provision: the “supply”, “acquisition”, “use”, or “sale” of harvested lists.[36] This provision should apply to all who aid, abet; counsel; procure; or induce, whether by threats or promises, or otherwise are in any way, directly or indirectly, knowingly concerned in, or conspire with others to contravene this provision.[37]

(f) Prohibition on the use of dictionary attacks

The Model Law should also prohibit the use of automated means to obtain e-mail addresses in order to initiate or advertise in an unsolicited electronic e-mail advertisement.[38] This prohibition should also extend to the use of scripts or other automated means to register for multiple e-mail accounts or online user accounts from which to transmit, or enable another person to transmit, commercial e-mail messages.[39] This provision must also include prohibition of the use of software and hardware for purposes of extracting personal information of recipients for spam purposes.[40]

(g) Enforcement and penalties

Regarding enforcement, consumers should be provided easy to follow methods in order to report spamming activities. These can include a web site where consumers can complain by leaving the names of those who are pestering them. In addition to fines and imprisonment, South Africa should implement mechanisms that can enforce the Act. As noted with the Australian experience the use of enforceable undertakings, and formal warnings have been effective in enforcing the Spam Act.

[36] See s 20; 21; 22 of the Spam Act; also s 17529.4 (a)(1) and (2) of the California Business and Professions Code; s 44-1372-01 (B) (2) (b) of the Arizona Revised Statutes; and section 3.805.1 of the Maryland Criminal Law Code.

[37] See s 20(5); 21 (3) and 22(3) of the Spam Act; and s 12 of the 2016 Cybercrimes Bill.

[38] See s 17529.4 (c) (1) and (2) of the California Business Professions Code.

[39] See s 5(b)(2) of the CAN-SPAM Act.

[40] See cl 6 of the 2015 Cybercrimes Bill; and s 2(2); 3; 4; 7 of the 2016 Cybercrimes Bill.

These measures will at least eliminate the time and costs that applicants have to expend in order to secure the prosecution of spammers.[41]

9.2.1.3 Conclusion

While the amendments to the current regime are welcomed, it should be remembered that legislation is but a starting point in ensuring that, at national level, spam is properly regulated and that safeguards for consumers are put in place. The remaining four multi-faceted approaches are outlined below.

9.2.2 Consumer education and awareness

9.2.2.1 Background

Consumer education should be the first priority in combating spam. An informed consumer is one who will act responsibly when engaging with technology and will ensure that he or she leaves minimal or no trail of personal information for marketers to exploit. As noted earlier, the majority of consumers in South Africa are uninformed as they were, by and large, excluded from the knowledge economy during the apartheid era. The preambles of the consumer oriented laws discussed in Chapter 8 also attest to this. Therefore, consumer education and awareness are vital to ensure that consumers are not only aware of their rights, but are also able to activate them. This type of education should be undertaken by all stakeholders, and here the Australian model, together with the recommendations of the ITU and OECD, would be particularly instructive.

9.2.2.2 The role of stakeholders in educating consumers

(a) Government

The role of the government is vital in this process, since it is instrumental in the type of education that can be offered at learning institutions. Although there is currently a

[41] These measures have proved efficient in Australia as part of its reporting process and it has apparently reduced the amount of spam within its borders. With the increase in spam, and especially SMS spam, this might prove effective in South Africa as an alternative measure.

subject on Information technology (IT) at grade school, that is only offered from grade 10 to 12 and not at all grade schools. And because it is only offered in the last years of grade school that means only a few learners will be exposed to such education. Besides, even the content of that subject is limited to specific IT issues. Considering that learners fall under the category of individuals who have access to smart phones, tablets et cetera, from an early age and that they use such efficiently than their caregivers, by the time they engage with IT issues they would have long been exposed to the dangers noted above.

It should therefore be the role of government to introduce IT subject that is age appropriate starting at the lower levels of grade school. This can form part of the existing subjects such as consumer studies, and even life orientation. At lower grades the content can start with an introduction to the basic functions of the devices that learners are already exposed to. This will then move on to the workings of the Internet and their activities in that environment, together with how their personal information can be compromised if they are not technologically savvy. The laws applicable in this arena should also be known to these young consumers. This will set the learners in the right direction towards being informed consumers.

Government should further ensure that the public at large is also exposed to this form of education through the media – for example, TV, information brochures, and even billboard advertisements. This education should be offered in all eleven official languages to ensure that all consumers are exposed to such information in the language they understand.

Government departments and institutions that deal with the dissemination of e-mails should also train their employees – in particular those directly involved in dealing with the processing of personal information. This education should also instruct employees on the dangers of accumulating or harvesting lists of personal information for sale.

(b) Internet service providers (ISP)

The ISPs role is very critical in that they are not only providing the devices but are also in a place to inform consumers with information that can assist such in safeguarding their activities while using their gadgets. The duty of the ISPs is to inform their customers to be technological savvy and not fall into traps set for them by marketers or scammers alike. This can be achieved through newsletters instructing customers on new technologies, the use of filters, basic security measures and other technological tools that the consumer can have access to in order to limit unsolicited communications.

In order to safeguard consumers' right to privacy, marketers should be compelled to adhere to the rules and regulations set out above. While these measures are sound, they will be of little avail if consumers remain ignorant on how to navigate the Internet and the laws in place to protect them. Education will allow consumers to make informed choices before engaging with marketers or accepting free-gift offers – as the adage goes "if it's free then you are the product".[42]

(c) Consumer advocacy groups

The issue of spam keeps on perpetuating because consumers keep on responding to spam by buying the products advertised. Therefore, consumer education and awareness should be seen as a key element which is important for the success of anti-spam legislation. Consumers should be in a position to know basic rules of online activities. These will include: how to limit their exposure to spam (by not leaving their e-mail addresses on numerous web sites); and where to complain when confronted with spam. The role of consumer advocacy groups can go a long way where consumers will be educated about their fundamental rights and how to respond in cases where those rights are infringed.

9.2.3 Industry initiatives

[42] See Techdirt 'Stop saying 'if you're not paying, you're the product'' https://www.techdirt.com/articles/20121219/18272921446/stop-saying-if-youre-not-paying-youre-products.shtml (date of use: 19 September 2016).

Industry should also be at the forefront in combating spam. Stakeholders such as: direct marketers; online operators; software companies; and ISPs should be setting examples as to how this should be done. Both the ISPA and DMASA are playing a vital role in combating spam. However, the codes of conduct of such industries should be in compliance with the founding legislation that established such an industry. These codes should take all technologies, new or future, into consideration and be amended as technology changes.

9.2.4 Technological measures

As noted above, filters have been at the forefront in limiting spam. However, they have also been shown to be limited in their application. As spammers find new ways to send spam, so should new technologies be developed and be made available to equip all stakeholders. The availability of new technological tools to customers has not only eliminated the middleman, but has also meant that consumers are available 24/7. This guarantees exposure to the marketers' all over the world. South Africa should look to the recommendations emanating from the international arena and align itself accordingly. Australia would be a good example here with the utilization of the SpamMatters button which enables consumers to report and delete spam at the same time.

9.2.5 International cooperation

Most spam in South Africa, originates from beyond its borders, and the laws are ill-equipped to prosecute those spammers. However, as the POPI Act addresses cross- border issues, it offers a starting point for dealing with these matters. Chapter 5 of the POPI Act mandates the Information Regulator to conduct research into this aspect and also to liaise with other Regulators on the application of the Act.

From these provisions South Africa should be in a position to conclude mutual agreements with countries notorious for sending spam, which will include the ten top worst countries from which the most spam is sent.[43] This will result in partnerships

[43] See Spamhaus 'The top 10 worst spam countries' https://www.spamhaus.org/statistics/countries (date of use: 12 March 2017). At the top of the

that would assist South Africa and those countries in dealing with spam beyond their respective borders, as a result holding one another accountable. These agreements should be extended to community blocks to which South Africa is a member, as well as other organisations interested in eliminating the scourge. This will save South Africa from the dubious ‘honour’ of becoming a safe haven for spammers and scammers alike. Having the type of measures identified above in place, would put South Africa in a position to best assist its consumers and bring perpetrators to book.

9.3 Recommendations and conclusion

South Africa has come a long way in developing laws in combating spam. The local and global nature of spam has been emphasized in this thesis and South Africa has attempted to accommodate these to some extent. It is, however, important to note that while South Africa has laws in place it is recommended that the country aligns its laws to protect its citizens by implementing an anti-spam law that can deal with the issue of spam decisively at national level. Once protection is in place nationally and stakeholders are playing their part in combating spam, then the next step will be to enter into mutual agreements with other countries and organisations in order to combat spam at a global level.

By so doing, South Africa would have aligned itself with international best practices that they strive to in their consumer oriented laws. While there is no guarantee that these measures will eradicate spam, as has been indeed noted in other jurisdictions – at least with such an alignment, local marketers and spammers alike will be compelled to adjust their behaviour to comply with the measures put in place. Consumers, on the other hand, would have received vital, albeit elusive, education to assist them in knowing how to navigate the technological space they find themselves in. As such, they will be informed consumers who will no longer be “the product” of spam and other fraudulent activities by marketers and spammers.

list is the United States; followed by China; Russian Federation; Hong Kong; Ukraine; Japan; United Kingdom; Germany; Turkey and India. All these are considered the worst spam haven countries.

For a healthy economy consumers need to be informed of the options available for them on how to fend for themselves before the law can even be put in place to protect them. Knowing their rights and responsibilities on how to use technology to their benefit will not only produce informed consumers but also well rounded consumers who are technologically savvy.

BIBLIOGRAPHY

BOOKS, DISSERTATIONS & THESIS

Asscher & Hoogcarspel *Regulating spam*

Asscher FL & Hoogcarspel SA *Regulating spam: A European perspective after the adoption of the E-Privacy Directive* (2006) Information Technology & Law Series (IT & Law 10)

Blainpain & Van Gestel *Use and monitoring of e-mail*

Blainpain R & Van Gestel M *Use and monitoring of e-mail, intranet and Internet facilities at work: law and practice* (Kluwer Law International 2004)

Cant & Van Heerden *Marketing management*

Cant MC & Van Heerden CH *Marketing management: A South African perspective* 2 ed (Juta & Co Ltd 2013)

De Bruin *Consumer trust*

De Bruin R *Consumer trust in electronic commerce: Time for best practice* (Kluwer Law International Netherlands 2002)

De Stadler *Consumer law*

De Stadler E *Consumer law unlocked* (SiberInk Cape Town 2013)

Downing, Covington & Covington *Dictionary*

Downing D, Covington M & Covington MM *Dictionary of computer and Internet Terms* 7 ed (Barron's 2000)

Feinstein *How to do everything*

Feinstein K *How to do everything to fight spam, viruses, pop-ups & spyware* (Corel VENTURAtm Publisher 2004)

Geissler *Bulk unsolicited electronic messages*

Geissler ML *Bulk unsolicited electronic messages (SPAM): A South African perspective* (LLD Thesis UNISA 2004)

Goodman *Spam wars*

Goodman D *Spam wars: Our last best chance to defeat spammers, scammers, and hackers* (SelectBooks Inc 2004)

Haase, Grimm & Versfeld *International commercial law*

Haase JW, Grimm N & Versfeld E *International commercial law from a South African perspective* (Shaker Aachen 2003)

Hitchcock *Net crimes*

Hitchcock JA *Net crimes and misdemeanors: Outmaneuvering web spammers, stalkers, and con artists* 2 ed (Information Today Inc 2006)

Hofman *Cyberlaw*

Hofman J *Cyberlaw: A guide for South Africans doing business online* (Stoddart Publishing Co Ltd 1999)

Kamal *Law of cyber-space*

Kamal A *The law of cyber-space: An invitation to the table of negotiations* (UNITAR 2005)

Kothari *Research Methodology: Methods and techniques*.

Kothari CR *Research Methodology: Methods and Techniques* (New Age International Publishers 2004)

Krum *Mobile marketing*

Krum C *Mobile marketing: Finding your consumers no matter where you are* (Pearson Education, Inc. 2010)

Maheeph *Electronic spamming*

Maheeph P *Electronic spamming within South Africa: A comparative analysis* (LLM Dissertation University of KwaZulu-Natal 2014)

Margolis *Computer & Internet dictionary*

Margolis PE *Computer & Internet dictionary* 3 ed (Random House NY 1998)

McQuid-Mason et al *Consumer law in South Africa*

McQuid-Mason D (gen ed) et al *Consumer law in South Africa* (Juta & Co Ltd Kenwyn 1997)

Naude & Eiselen *Commentary*

Naude T & Eiselen T (eds) *Commentary on Consumer Protection Act* (Juta & Co (Pty) Ltd Claremont 2014)

Neethling, Potgieter & Visser *Neethling's Law of personality*

Neethling J, Potgieter JM & Visser PJ *Neethling's Law of personality* 2 ed (LexisNexis Durban 2007)

Opperman & Lake *Understanding the CPA*

Opperman I & Lake R *Understanding the Consumer Protection Act* (Juta & Co Ltd Cape Town 2012)

Oxford *Dictionary of computer science*

Oxford *A Dictionary of computer science* 7 ed (Oxford University Press NY USA 2016)

Poteet *Canning spam*

Poteet J *Canning spam: You've got mail (that you don't want)* (SAMS 2004)

Roos *Law of Data protection*

Roos A *The law of data (privacy) protection: A comparative and theoretical Study* (LLD Thesis UNISA 2003)

Rowles *Mobile Marketing*

Rowles D *Mobile marketing: How mobile technology is revolutionizing marketing, communications and advertising* 1 ed. (Kogan Page Limited London 2014)

Scholtz et al *Guide to National Credit Act*

Scholtz JW et al *Guide to the National Credit Act* (LexisNexis South Africa 2008)

Schryen *Anti-spam measures*

Schryen G *Anti-spam measures: Analysis and design* (Springer-Verlag 2007)

Simmons & Simmons *E-commerce law*

Simmons & Simmons Communications *E-commerce law: Doing business online* (Palladian Law Publishing Ltd 2001)

Shostak *The cyberunion*

Shostak AB (ed) *The cyberunion handbook: Transforming labor through computer technology* (ME Sharpe Armonk New York 2002)

Sterne & Priore *Email marketing*

Sterne J & Priore A *email marketing: Using email to reach your target audience and build consumer relationships* (John Wiley & Sons Inc 2000)

Van Eeden *Consumer protection law*

Van Eeden E *Consumer protection law in South Africa* (LexisNexis South Africa 2013)

Van Schalkwyk & Marlie *Transactions of the Centre for business law*

Van Schalkwyk LM & Marlie L *The protection of commercial information in electronic communications with special reference to the Internet* (UV/UFS Bloemfontein 2005)

Walker *Absolute beginners guide*

Walker A *Absolute beginners guide to security spam spyware and viruses* 2 ed (QUE Indianapolis Indiana 2006)

York & Chia *E-commerce*

York S & Chia K (eds) *E-commerce: A guide to the law of electronic business* (Butterworths London 1999)

Zdziarski *Ending spam*

Zdziarski J.A *Ending spam: Bayesian content filtering and the art of statistical language classification* (No Starch Press San Francisco 2005)

CHAPTERS IN BOOKS

Buys ‘Online consumer protection and spam’

Buys R ‘Online consumer protection and spam’ in Buys R & Cronjé F (eds) *Cyberlaw @ SA II: The Law of the Internet* 2 ed (Van Schaik Publishers Pretoria 2004) 138-70

Buys ‘Privacy and the right to information’ 365-91

Buys R ‘Privacy and the right to information’ in Buys R (ed) *Cyberlaw @ SA: The Law of the Internet* 1 ed (Van Schaik Publishers Pretoria 2000) 365-91

Bwalya ‘E-commerce penetration’

Bwalya KJ ‘E-commerce penetration in the SADC region: Consolidating and moving forward’ in Cruz-Cunha MM & Varajao J (eds) *E-business Managerial Aspects, Solutions and Case Studies* (Hershey, Pa: IGI Global 2011) 235-53

Collier D ‘Criminal law and the Internet’

Collier D ‘Criminal law and the Internet’ in Buys R (ed.) *Cyberlaw @ SA II: The Law of the Internet* (2004) 319-347

Du Plessis ‘The African Union’

Du Plessis M ‘The African Union’ in Dugard J *International Law: A South African Perspective* 3 ed (Juta & Co Ltd Lansdowne SA 2006) 546-54

Eiselen ‘E-commerce’

Eiselen S ‘E-commerce’ in Van der Merwe D (ed) *Information and Communications Technology Law* 2 ed. (Lexis Nexis Durban 2016) 149-220

Gereda ‘The Electronic Communications and Transaction Act’

Gereda SL ‘The Electronic Communications and Transaction Act’ in Thornton et al (eds) *Telecommunications Law in South Africa* (STE Publishers Johannesburg 2006) 262-95

Goodburn & Ngoye ‘Privacy and the Internet’

Goodburn D & Ngoye M ‘Privacy and the Internet’ in Buys R & Cronjé F (eds) *Cyberlaw @ SA II: The Law of the Internet* 2 ed (Van Schaik Publishers Pretoria 2004) 171-96

Gordon ‘Internet criminal law’

Gordon B ‘Internet criminal law’ in *Cyberlaw @ SA: The law of the Internet* (2000) 423-446

Groenewald ‘Towards an electronic commerce policy for South Africa’

Groenewald M ‘Towards an electronic commerce policy for South Africa’ in Buys (ed) *Cyberlaw @ SA: The Law of the Internet* (Van Schaik Publishers Pretoria 2000) 97-113

Meiring ‘Electronic transactions’

Meiring R ‘Electronic transactions’ in Buys R & Cronjé F (eds) *Cyberlaw @ SA II: The Law of the Internet* 2 ed (Van Schaik Publishers Pretoria 2004) 82-108

Papadopoulos ‘Online consumer protection’

Papadopoulos S ‘Online consumer protection’ in Papadopoulos S & Snail S (eds) *Cyberlaw @ SA*: *Law of the Internet* 3 ed (Van Schaik Publishers 2012) 63-93

Papadopoulos & Snail ‘Privacy and protection’

Papadopoulos S & Snail S Privacy and protection’ in Papadopoulos S & Snail S (eds) *Cyberlaw @ SA*: *Law of the Internet* 3 ed (Van Schaik Publishers 2012) 275-313

Roos A ‘Data Protection’

Roos A ‘Data Protection’ in Van der Merwe D (ed) *Information and Communications Technology Law* (LexisNexis South Africa 2008) 313-97

Roos ‘Data Privacy Law’

Roos A ‘Data Privacy Law’ in Van der Merwe D (ed.) *Information and Communications Technology Law* 2nd ed. (LexusNexis 2016) 363-487

Tladi S ‘SPAM: An overview’

Tladi S 'SPAM: An overview of South African legislative development' in Kierkegaard S (ed) *Law & Practice Critical Analysis and Legal Reasoning* (International Association of IT Lawyers 2013) 266-78

Van der Merwe D 'Criminal Law'
Van der Merwe D 'Criminal Law' in Van der Merwe D (ed) *Information and Communications Technology Law* (LexisNexis South Africa 2008) 61-102

Watney 'Cybercrime and the investigation of cybercrime'
Watney M 'Cybercrime and investigation of cybercrime' in *Cyberlaw @ SA: The law of the Internet* (2012) 333-51

JOURNAL ARTICLES

Albrecht (2002-2003) 36 *Suffolk University Law Review*
Albrecht LJ 'Online marketing: The use of cookies and remedies for Internet users' (2002-2003) 36 *Suffolk University Law Review* 421-49

Alepin (2004-2005) 28 *Columbia Journal of Law & the Arts*
Alepin DC 'Opting-out: a technical, legal and practical look at the CAN-SPAM Act of 2003' (2004-2005) 28 *Columbia Journal of Law & the Arts* 41-70

Alongi (2004) 46 *Arizona Law Review*
Alongi EA 'Has the US canned spam' (2004) 46 *Arizona Law Review* 263-290

Amaditz (1999) *Virginia Journal of Law and Technology*
Amaditz KC 'Canning 'spam' in Virginia: Model legislation to control junk e-mail' 1999 *Virginia Journal of Law and Technology* 4 http://www.vjolt.net/vol4/issue/home_art4.html (Date of use: 30 December 2015)

Ampratwum (2009) 16/1 *Journal of Financial Crime*
Ampratwum EF 'Advance fee fraud '419' and investor confidence in the economies of sub-Saharan Africa (SSA)' (2009) 16/1 *Journal of Financial Crime* 67-80

Atta-Asamoah (2009) 18/4 *African Security Review*
Atta-Asamoah A 'Understanding the West African cyber crime process' (2009) 18/4 *African Security Review* 106-114

Balough (2003) 22/1 (Fall) *John Marshall Journal of Computer and Information Law*
Balough RC 'The Do-Not-Call Registry Model is not the answer to spam' (2003) 22/1 (Fall) *John Marshall Journal of Computer and Information Law* 79-96

Baxter (2004) 8 1 *NYU Journal of Legislation and Public Policy*
Baxter P.W 'Has Spam Been Canned: consumers, marketers, and the making of the CAN-SPAM Act 2003' (2004) 8/1 *NYU Journal of Legislation and Public Policy* 163-178

Bennett (2011) 44/4 *John Marshall Law Review*
Bennett S 'Regulating online behavioural advertising' (2011) 44/4 *John Marshall Law Review* 899-962

Bindman (2013) 39/4 *William Mitchell Law Review*

Bindman JC 'The spam filter ate my e-mail: When are electronic records received?' (2013) 39/4 *William Mitchell Law Review* 1295-1332

Bolin (2006) 24/2 *Yale Law and Policy Review*

Bolin R 'Opting out of spam: A domain level do-not-spam registry' (2006) 24/2 *Yale Law and Policy Review* 399-435

Bowman (2012) 7/3 *Journal of Law and Policy for the Information Society*

Bowman LJ 'Pulling back the curtain: Online consumer tracking' (2012) 7/3 *Journal of Law and Policy for the Information Society* 721-52

Brandon (2012) 29/1 *John Marshall Journal of Computer and Information*

Brandon SC 'What's mine is yours: Targeting privacy issues and determining the best solutions for behavioral advertising' (2012) 29/1 *John Marshall Journal of Computer and Information* 637-72

Brockhoeft (2004) 4 *Loyola Law and Technology Annual*

Brockhoeft J.E 'Evaluating the CAN-SPAM Act of 2003' (2004) 4 *Loyola Law and Technology Annual* 1-44

Budnitz (1998) 49/4 *South Carolina Law Review*

Budnitz ME 'Privacy protection for consumer transactions in electronic commerce: Why self-regulation is inadequate' (1998) 49/4 *South Carolina Law Review* 847-86

Burger & Rensleigh (2007) 9/3 *South African Journal of Information Management*

Burger E & Rensleigh C 'Investigating e-mail overload in South African banking industry' (2007) 9/3 *South African Journal of Information Management* 1-18 http://www.sajim.co.za/default.asp?to=peer1vol9nr3 (date of use: 7 September 2015)

Cain (2007-2008) 3 *I/S: Journal of Law and Policy for the Information Society*

Cain RM 'When does pre-emption not really pre-empt? The role of state law after CAN-SPAM' (2007-2008) 3 *I/S: Journal of Law and Policy for the Information Society* 751-76

Canfield (2009-2010) 20 *Civil Rights Law Journal*

Canfield N.S 'The fallacy of publius as spammer: Jaynes v Commonwealth of Virginia and the proper doctrine for reviewing state anti-spam laws' (2009-2010) 20 *Civil Rights Law Journal* 449-470

Cassim (2010) 5/3 *Journal of International Commercial Law and Technology*

Cassim F 'Addressing the challenges posed by cybercrime: a South African perspective' (2010) 5/3 *Journal of International Commercial Law and Technology* 118-23

Cassim (2011) 44/1 *CILSA*

Cassim F 'Addressing the growing spectre of cybercrime in Africa: Evaluating measures adopted by South Africa and other regional role players' (2011) 44/1 *CILSA* 123-38

Cassim (2014) 47/3 *CILSA*

Cassim F 'Addressing the spectre of phishing: Are adequate measures in place to protect victims of phishing?' (2014) 47/3 *CILSA* 401-28

Chapman (2007) 30/1 *UNSW Law Journal*

Chapman C 'The legal challenges facing ACMA as Regulator' (2007) 30/1 *UNSW Law Journal* 220-31

Coetzee (2004) 3 *Stell LR*

Coetzee J 'The Electronic Communications and Transactions Act 25 of 2002: facilitating electronic commerce' (2004) 3 *Stell LR* 501-21

Dane (2006) 6 *Asper Review of International Business & Trade Law*

Dane K 'Controlling spam: the prospect of legislative success' (2006) 6 *Asper*
Review International Business & Trade Law 241-64

Daniel (2005-2006) 94 *Kentucky Law Journal*

Daniel JW 'Has spam been fried? Why CAN-SPAM Act of 2003 can't: Regulation of unsolicited commercial electronic mail and the CAN-SPAM Act of 2003' (2005-2006) 94 *Kentucky Law Journal* 363-92

De Villiers (2007) Oct/Nov *Journal of Marketing*

De Villiers D 'The opt-in vs opt-out debate' (2007) Oct/Nov *Journal of Marketing* 19-20

Dickinson (2004) 57/1 *Federal Communications Law Journal*

Dickinson D 'An architecture for spam regulation (2004) 57/1 *Federal Communications Law Journal* 129-60

Du Preez (2009) 1 *TSAR*

Du Preez M.L 'The Consumer Protection Bill: a few preliminary comments' (2009) 1 *TSAR* 58-83

Ebersöhn (2003) July *De Rebus*

Ebersöhn G 'The unfair business practices of spamming and spoofing' (2003) July *De Rebus* 25-6

Ebersöhn (2004) 16/4 *SA Merc LJ*

Ebersöhn G 'Internet law: cookies, traffic data, and direct advertising practices' (2004) 16/4 *SA Merc LJ* 741-64

Ebersöhn (2004) 12/3 *JBL*

Ebersöhn G 'An analysis of spam regulation: developments in America, Australia, and Europe' (2004) 12/3 *JBL* 137-42

Engle (2007-2008) 3/3 *Journal of Law and Policy for the Information Society*

Engle MM 'Anti-spyware enforcement: recent developments' (2007-2008) 3/3 *Journal of Law and Policy for the Information Society* 581-94

Esselaar & Miller (2002) 2/1 *South African Journal of information and Communication*

Esselaar P & Miller J 'Towards electronic commerce in Africa: A perspective from three country studies' (2002) 2/1 *South African Journal of information and Communication* 1-12 http://www.sajic.org.za/index.php/SAJIC/20%article/20%viewArticle/172 (date of use: 27 December 2015)

Ewelukwa (2011) 13 *European Journal of Law Reform*

Ewelukwa N 'Is Africa ready for electronic commerce: A critical appraisal of legal framework for ecommerce in Africa' (2011) 13 *European Journal of Law Reform* 550-76

Fagan (2004) 33/10 *Colorado Lawyer*

Fagan M 'Practicing safe e-mailing: The CAN-SPAM Act of 2003' (2004) 33/10 *Colorado Lawyer* 61-6

Fingerman (2004) 7/8 *Journal of Internet law*

Fingerman D 'Spam canned throughout the land? Summary of the CAN-SPAM Act commentary' (2004) 7/8 *Journal of Internet law* 1-14 http://www.danfingerman.com/papers/CAN-SPAM.doc (date of use: 30 December 2015)

Fleming & O'Carroll (2010) 16/4 *Parallax*

Fleming C and O'Carroll J 'The art of the hoax' (2010) 16/4 *Parallax* 45-59

Gereda 2003 *De Rebus*

Gereda S 'The truth about spam' (2003) *De Rebus* 51-2

Glickman (2005) 39/3 *Canadian Journal of African Studies*

Glickman H 'The Nigerian '419' advance fee scams: Prank or peril?' (2005) 39/3 *Canadian Journal of African Studies* 460-89

Goldman (2003) 22 *John Marshall Journal of Computer and Information Law*

Goldman E 'Where's the beef? Dissecting spam's purported harms' (2003) 22 *John Marshall Journal of Computer and Information Law* 13-28

Greenleaf & Georges (2014) 132 *Privacy Laws and Business International Report*

Greenleaf G & Georges M 'African regional privacy instruments: Their effects on harmonization' (2014) 132 *Privacy Laws and Business International Report* 19-21 http://papers.ssrm.com (date of use: 31 December 2015)

Grossman (2004) 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* 1533-76

Hamman & Papadopoulos (2014) 47/1 *De Jure*

Hamann B & Papadopoulos S 'Direct marketing and spam via electronic communications: an analysis of the regulatory framework in South Africa' (2014) 47/1 *De Jure* 42-62

Helman (2009) 50 *Boston College Law Review*

Helman I 'Spam-a-lot: the states' crusade against unsolicited e-mail in light of the CAN-SPAM Act and the overbreadth doctrine' (2009) 50 *Boston College Law Review* 1525-62

Hoofnagle et al (2012) 6 *Harvard Law and Policy Review*

Hoofnagle et al 'Behavioral advertising: The offer you cannot refuse' (2012) 6 *Harvard Law and Policy Review* 273-96

Ider (1999) 138/7 *Trusts and Estates*

Idler J 'Protecting your right to privacy on the Internet' (1999) 138/7 *Trusts and Estates* 41-5

Irving (1996) 1 *University of Chicago Legal Forum*

Irving L 'Safeguarding consumers' interests in cyberspace' (1996) 1 *University of Chicago Legal Forum* 1-14

Jacobs (2004) 16/4 *SA Merc LJ*

Jacobs W 'The Electronic Communications and Transactions Act: Consumer
protection and Internet contract' (2004) 16/4 *SA Merc LJ* at 556-67

Jacobs, Stoop & Van Niekerk (2010) 13/3 *PER PELJ*

Jacobs W, Stoop P, & Van Niekerk R 'Fundamental consumer rights under the Consumer Protection Act 68 of 2008: A critical overview and analysis' (2010) 13/3 *PER PELJ* 302-406

Jansen van Ryssen (2004) 4 *Acta Commercii*

Jansen van Ryssen F 'SMS marketing: It's place in mobile commerce and opportunity in the South African Market' (2004) 4 *Acta Commercii* 48-59

Jayamala (2014) 95/1131 *Australian Journal of Pharmacy*

Jayamala G 'Scams: It's a scam' (2014) 95/1131 *Australian Journal of Pharmacy* 18-19 http://search.informit.com.au/fullText;dn=759638788394502;res=IELHEA (date of use: 6 November 2015)

Jobodwana (2009) 4 *Journal of International Law and Technology*

Jobodwana NT 'E-commerce and mobile commerce in South Africa: Regulatory challenges' (2009) 4 *Journal of International Law and Technology* 287-98

Jordaan (2007) 3/1 *International Retail and Marketing Review*

Jordaan Y 'Information privacy issues: implications for direct marketing' (2007) 3/1 *International Retail and Marketing Review* 42-53

Jordaan & Jordaan (2004) 23/1 *Journal for Communication Sciences in Southern Africa*

Jordaan Y & Jordaan AC 'Communicating the protection of information privacy' (2004) 23/1 *Journal for Communication Sciences in Southern Africa* 137-48

Kendrick (2003 Fall) 7/3 *Journal of Small and Emerging Business Law*

Kendrick JP 'Subject: ADV: Anti-spam laws force emerging Internet business advertisers to wear the scarlet 'S'' (2003) 7/3 (Fall) *Journal of Small and Emerging Business Law* 563-76

Kennedy (2009) Aug/Sept *Journal of Marketing*

Kennedy C 'SMS competitions: are they one big rip-off?' (2009) Aug/Sept *Journal of Marketing* 22-3

Kent (2004) 76/4 *Australian Quarterly*

Kent M 'Spam regulation and Australia: National sovereignty and the .au' (2004) 76/4 *Australian Quarterly* 4-5 and 40

Khong (2004) 1 *Erasmus Law and Economic Review*

Khong WK 'An economic analysis of spam laws' (2004) 1 *Erasmus Law and Economic Review* 23-45

Kikuchi (2004) 10/2 *BUJ Sci & Tech L*

Kikuchi EH 'Spam a box: Amending CAN-SPAM & aiming toward a global solution' (2004) 10/2 *BUJ Sci & Tech L* 263-325

King (2003) 12 *Information and Communications Technology Law*

King I 'On-line privacy in Europe-new regulation for cookies' (2003) 12 *Information and Communications Technology Law* 224-36

Kokt & Koelane (2013) 7/31 *African Journal of Business Management*

Kokt D & Koelane T 'Reflecting on information and communication and technology (ICT) in marketing from a marketer's and student perspective' (2013) 7/ 31 *African Journal of Business Management* 3098-3108

Lanois (2010) 9/2 *Northwestern Journal of Technology and Intellectual Property*

Lanois P 'Caught in the clouds: The web 2.0, cloud computing, and privacy?' (2010) 9/2 *Northwestern Journal of Technology and Intellectual Property* 29-50

Lavergne (2005) 1/3 *NYU Journal of Law & Business*

Lavergne EN 'FCC gives teeth to CAN-SPAM Act of 2003' (2005) 1/3 *NYU Journal of Law & Business* 861-80

Ledbetter (2004) 34 *Southwestern University Law Review*

Ledbetter TK 'Stopping unsolicited commercial e-mail: Why the CAN-SPAM Act is not the solution to stop spam' (2004) 34 *Southwestern University Law Review* 107-32

Leiserson (2002) 94/3 *Law Library Journal*

Leiserson AB 'A user's perspective on privacy and web' (2002) 94/3 *Law Library Journal* 539-46

Li (2006) 3/1 *Webology*

Li X 'E-marketing, unsolicited commercial e-mail, and legal solutions' (2006) 3/1 *Webology* http://webology.ir/2006/v3n1/a23.html (date of use: 5 November 2015) 1-13

Lindner & Riehm (2009) 1/1 *JeDEM*

Lindner R & Riehm U 'Electronic petitions and institutional modernization: international parliamentary e-petition systems in comparative perspective' (2009) 1/1 *JeDEM* 1-11 http://www.itas.kit.edu/pub/v/2009/liri09a.pdf (date of use: 6 November 2015)

Lorentz (2011) 30/3 *Review of Litigation*

Lorentz D 'The effectiveness of litigation under the CAN-SPAM Act' (2011) 30/3 *The Review of Litigation* 559-606

Machacek (2011) 14 *Chapman Law Review*

Machacek MS 'Digest: Kleffman v Vonage Holdings Corp' (2011) 14 *Chapman Law Review* 583-8

Magaqa (2015) 27/1 *SA Merc LJ*

Magaqa M 'The NCC and the NCT walk the long road to consumer protection' (2015) 27/1 *SA Merc LJ* 32-57

Magee (2003) 19/2 *Santa Clara Computer and High Technology Law Journal*

Magee J 'The law regulating unsolicited commercial e-mail: An international perspective' (2003) 19/2 *Santa Clara Computer and High Technology Law Journal* 333-82

Malcolm (2001) 12/2 *Journal of Law and Information Science*

Malcolm J 'Recent developments in Australian spam laws' (2001) 12/2 *Journal of Law and Information Science* 242-58

Manwaring (2009) *Computers and Law*

Manwaring K 'Canning the spam five years on: A comparison of spam regulation in Australia and the US' (2009) *Computers and Law* 5-11

Marks (2004) 54/3 *Case Western Reserve Law*

Marks EE 'Spammers clog in-boxes everywhere: Will the CAN-SPAM Act of 2003 halt the invasion? (2004) 54/3 *Case Western Reserve Law* 943-63

Marx & O'Brien (2011) 32/3 *Obiter*

Marx FE & O'Brien N 'To regulate or to over-regulate: Internet service provider liability: The industry representative body in terms of the ECT Act and regulations' (2011) 32/3 *Obiter* 537-56

Mayer (2004) 31/1 *Journal of Legislation*

Mayer DL 'Attacking a windmill: Why the CAN-SPAM Act is a futile waste of time and money' (2004) 31/1 *Journal of Legislation* 177-90

McQuoid-Mason (1982) XV/1 *CILSA*

McQuoid-Mason D 'Consumer protection and the right to privacy' (1982) XV/1 *CILSA* 135-57

Mercado-Kierkegaard (2005) 21/4 *Computer Law & Security Report*

Mercado-Kierkegaard S 'How the cookie (almost) crumbled: Privacy & lobbyism' (2005) 21/4 *Computer Law & Security Report* 310-22

Meyerowitz (2008) *Privacy & Data Security Law Journal*

Meyerowitz SA 'Virginia Supreme court rejects state's anti-spam law on First Amendment grounds' (2008) *Privacy & Data Security Law Journal* 1024-1042 http://www.meyerowitzcommunications.com/pdf/Meyerowitz%20Spam%20Ruling.pdf (date of use: 30 December 2015)

Mobarek (2004) 16/3 *Loyola Consumer Law Review*

Mobarek SI 'The CAN-SPAM Act of 2003: Was congress actually trying to solve the problem or add to it?' (2004) 16/3 *Loyola Consumer Law Review* 247-66

Monty (2015) 15/6 *Without Prejudice*

Monty S 'The popping of POPI' (2015) 15/6 *Without Prejudice* 86-7

Mossoff (2004) 19/2 *Berkley Technology Law Journal*

Mossoff A 'Spam, oy what a nuisance!' (2004) 19 2 *Berkley Technology Law Journal* 625-66

Motloung (2015) March *IMM Journal of Strategic Marketing*

Motloung M Big data is all about gut feel and common sense' (2015) March *IMM Journal of Strategic Marketing* 18-19

Mudelair (2008) *Journal of Marketing*

Mudelair T 'Opting-out' (2008) *Journal of Marketing* 22-3

Mutchler (2010) 43 *Suffolk University Law Review*

Mutchler A 'CAN-SPAM versus the European Union E-Privacy Directive: Does either provide a solution to the problem of spam?' (2010) 43 *Suffolk University Law Review* 957-81

Naude & Papadopoulos (2016) 79/1 *THRHR*

Naude A & Papadopoulos S 'Data Protection in South Africa: The Protection of Personal Information Act 4 of 2013 in light of recent international developments (1)' (2016) 79/1 *THRHR* 51-68

Naude & Papadopoulos (2016) 79/2 *THRHR*

Naude A & Papadopoulos S 'Data Protection in South Africa: The Protection of Personal Information Act 4 of 2013 in light of recent international developments (2)' (2016) 79/2 *THRHR* 213-230

Ndonga (2012) 5 *African Journal of Legal Studies*

Ndonga D 'E-Commerce in Africa: challenges and solutions' (2012) 5 *African Journal of Legal Studies* 243-68

Neels (2010) 31/1 *Obiter*

Neels JL 'Consumer protection legislation and private international law' (2010) 31/1 *Obiter* 122-33

Neethling (2012) 75 *THRHR*

Neethling J 'Features of the Protection of Personal Information Bill' (2012) 75 *THRHR* 241-55

Nelson (2003) 58 *Business Lawyer*

Nelson VA 'Use of UCE: State laws regarding unsolicited commercial e-mail advertisements' (2003) 58 *The Business Lawyer* 1203-14

O'Neill (2001) 47 *Consumer Interests*

O'Neill B 'Online Shopping: Consumer Protection and Regulation' (2001) 47 *Consumer Interests* 1-3

Papadopoulos (2012) 75 *THRHR*

Papadopoulos S 'Are we about to cure the scourge of spam: A commentary on current and proposed South African legislative intervention' (2012) 75 *THRHR* 223-40

Petzer (2011) 8 *Journal of Contemporary Management*

Petzer DJ 'Investigating mobile marketing acceptance of urban South Africans residing in Gauteng' (2011) 8 *Journal of Contemporary Management* 384-407

Pillay (2014) 14/8 *Without Prejudice*

Pillay L 'The partial commencement of the Protection of Personal Information Act 2013' (2014) 14/8 *Without Prejudice* 54

Pistorius & Tladi (2014) 26/3 *SA Merc LJ*

Pistorius T & Tladi SEM 'The hall of shame: Double standards for spam' (2014) 26/3 *SA Merc LJ* 688-705

Prince & Shea (2003) 22 *John Marshall Journal of Computer & Information Law*

Prince M & Shea PA 'After CAN-SPAM: How states can stay relevant in the fight against unwanted messages: How children's protection registry can be effective and is not pre-empted under the new federal anti-spam law' (2003) 22 *John Marshall Journal of Computer & Information Law* 29-78

Quo (2004) 11/1 *Murdoch University Electronic Journal of Law*

Quo S 'Spam: Private and legislative responses to unsolicited electronic mail in Australia and United States' (2004) 11/1 *Murdoch University Electronic Journal of Law* 1-31 http://www.austlii.edu.au/au/journals/MurUEJL/2004/11.html (date of use: 15 January 2016)

Reid (2010) 4/2 *Akron Intellectual Property Journal*

Reid VJ 'Recent developments in private enforcement of the CAN-SPAM Act' (2010) 4/2 *Akron Intellectual Property Journal* 281-308

Relf (2005) 2 *Macquarie J Bus L*

Relf P 'A look at Australia's new anti-spam legislation' (2005) 2 *Macquarie J Bus L* 91-118

Renke, Roestoff, & Haupt (2007) 28/2 *Obiter*

Renke S, Roestoff M & Haupt F 'The National Credit Act: New parameters for granting of credit in South Africa' (2007) 28/2 *Obiter* 229-70

Rogers (2004) 25 *Business Law Review*

Rogers KM 'The Privacy Directive and resultant regulations: The effect on spam and cookies Part II' (2004) 25 *Business Law Review* 271-74

Roos (2006) 39/1 *CILSA*

Roos A 'Core principles of data protection law' (2006) 39 1 *CILSA* 103-30

Roos (2007) 124/2 *SALJ*

Roos A 'Data protection: explaining the international backdrop and evaluating the current South African position' (2007) 124/2 *SALJ* 400-37

Roos (2008) 4 *PELJ*

Roos A 'Personal data protection in New Zealand: lessons for South Africa?' (2008) 4 *PELJ* 62-109

Rothchild (1999) 74/3 *Indiana Law Journal*

Rothchild J 'Protecting the digital consumer: The limits of cyberspace utopianism' (1999) 74/3 *Indiana Law Journal* 893-989

Rutenberg (2011-2012) 14/1 *Vanderbilt Journal of Entertainment and Technology Law* Rutenberg D.J 'Silence of the spam: Improving the CAN-SPAM Act by including an expanded private cause of action' (2011-2012) 14/1 *Vanderbilt Journal of Entertainment and Technology Law* 225-52

Saurombe (2009) 21 *SA Merc LJ*

Saurombe A 'The SADC Trade Agenda, a tool to facilitate regional commercial law: An analysis' (2009) 21 *SA Merc LJ* 695-709

Schryen (2007) 16/1 *Information and Communications Technology Law*

Schryen G 'Anti-Spam Legislation: An analysis of laws and their effectiveness' (2007) 16/1 *Information and Communications Technology Law* 17-32

Shames (2004) 66 *University of Pittsburgh Law Review*

Shames ME 'Congress opts out of canning spam' (2004) 66 *University of Pittsburgh Law Review* 385-410

Slutsky & Baran (2005) 10 *Georgia Bar Journal*

Slutsky B & Baran S 'Spyware and the Internet: A cyberspace odyssey' (2005) 10 *Georgia Bar Journal* 22-5

Smith (2009) 23/1 *Cultural Studies*

Smith A 'Nigerian scam e-mails and the charms of capital' (2009) 23/1 *Cultural Studies* 27-47

Smith (2004) 16 *SA Merc LJ*

Smith A 'Privacy and the sale of customer lists in South African Insolvency law: Some issues reconnoiteres' (2004) 16 *SA Merc LJ* 598-621

Smith (2005) 12/2 *Competition and Consumer Law Journal*

Smith L 'Global online shopping: How well protected is the Australian consumer?' (2005) 12/2 *Competition and Consumer Law Journal* 163-90

Snail (2007) 15/2 *JBL*

Snail L 'An overview of South African e-consumer law in the context of the Electronic Communications and Transactions Act (part 2)' (2007) 15/2 *JBL* 54-60

Snail (2009) 1 *Journal of Information Law & Technology*

Snail S 'Cyber-crime in South Africa: Hacking, cracking, and other unlawful online activities' (2009) 1 *Journal of Information Law & Technology* 1-13 http://go.warwick.ac.uk/jilt/2009_1/snail (date of use: 28 January 2016)

Sibanda (2008) 1 *Journal of Information Law & Technology*

Sibanda OS 'Anti-spam: a comparative appraisal of Canadian, European Union, and South African regulatory regimes' (2008) *Journal of Information Law & Technology* 1-9 http://go.warwick.ac.uk/jilt/2008_2/sibanda (date of use: 20 January 2016)

Soma, Singer & Hurd (2008) 45 *Harvard Journal on Legislation*

Soma J, Singer P, & Hurd J 'Spam still pays: The failure of the CAN-SPAM Act of 2003 and proposed legal solutions' (2008) 45 *Harvard Journal on Legislation* 165-98

Sorkin (2001) 35/2 *University of San Fransisco Law Review*

Sorkin DE 'Technical and legal approaches to unsolicited e-mail' (2001) 35/2 *University of San Fransisco Law Review* 325-84

Sorkin (2003) 22/1 *John Marshall Journal of Computer and Information Law*

Sorkin DE 'Spam legislation in the United States' (2003) 22/1 *John Marshall Journal of Computer and Information Law* 3-12

Stein (2012) 12/10 *Without Prejudice*

Stein P 'South Africa's EU-style data protection law' (2012) 12/10 *Without Prejudice* 48-9

Steindel (2011) 17/2 *Michigan Telecommunications and Technology Law Review*

Steindel TA 'A path toward user control of online profiling' (2011) 17/2 *Michigan Telecommunications and Technology Law Review* 459-90

Subramaniam, Jalab HA & Taqa AY (2010) 5/12 *International Journal of the Physical Sciences*

Subramaniam T, Jalab HA & Taqa AY 'Overview of textual anti-spam filtering techniques' (2010) 5/12 *International Journal of the Physical Sciences* 1869-82 http://www.academicjournals.org/app/webroot/article/article1380815369_Subramaniam%20et%20al.pdf (Date of use: 26 November 2015)

Susuk (2010) 6/2 *Washington Journal of Law Technology and Arts*

Susuk L 'Death of the spam wrangler: CAN-SPAM private plaintiffs required to show actual harm' (2010) 6/2 *Washington Journal of Law Technology and Arts* 155-69

Swales (2016) 28/1 *SA Merc LJ*

Swales L 'Protection of personal information: South Africa's answer to the global phenomenon in the context of unsolicited electronic messages (spam)' (2016) 28/1 *SA Merc LJ* 49-84

Szabo (2006) 7 *Texas Review of Entertainment & Sports Law*

Szabo C.M 'Attempting to herd spam and the effects of *White Buffalo Ventures, LLC v University of Texas at Austin*' (2006) 7 *Texas Review of Entertainment & Sports Law* 63-78

Tladi (2008) 125/1 *SALJ* 178-92

Tladi S 'The Regulation of unsolicited commercial communications (spam): Is the opt-out mechanism effective?' (2008) 125/1 *SALJ* 178-92

Traung (2010) 31/10 *Business Law Review*

Traung P 'EU law on spyware, web bugs, cookies, etc., revisited: Article 5 of the Directive on Privacy and Electronic Communications' (2010) 31/10 *Business Law Review* 216-28

Trussell (2004) 16/2 *Loyola Consumer Law Review*

Trussell J 'Is the CAN-SPAM Act the answer to the growing problem of spam?' (2004) 16/2 *Loyola Consumer Law Review* 175-88

Uchenna (2012) 17/4 *Journal of Computer and Telecommunications Law*
Uchenna JO 'A discourse on the perceived defects of the draft African Union Convention on the Establishment of a Credible Legal Framework for Cybersecurity' (2012) 17/4 *Journal of Computer and Telecommunications Law* 128-30

Vaile (2004) 6/9 *Internet Law Bulletin*
Vaile D 'Spam canned: new laws Australia' (2004) 6/9 *Internet Law Bulletin* 113-15

Volker (2011-2012) Summer *Auditing*
Volker E 'Ponzi schemes in South Africa: a practical discussion' (2011-2012) Summer *Auditing SA* 5-10

Warner (2003) 22 *John Marshall Journal of Computer and Information Law*
Warner R 'Spam and beyond: freedom, efficiency, and the regulation of e-mail advertising' (2003) 22 *John Marshall Journal of Computer and Information Law* 141-77

Whipple (2013) 21 *LBJ Journal of Public Affairs*
Whipple M 'Regulating consumer profiling: going beyond advertising' (2013) 21 *LBJ Journal of Public Affairs* 89-129

Woker (2010) 31/2 *Obiter*
Woker T 'Why the need for consumer protection legislation: a look at some of the reasons behind the promulgation of the National Credit Act and the Consumer Protection Act' (2010) 31/2 *Obiter* 217-23

Wong (2007) 20/2 *Harvard Journal of Law & Technology*
Wong K 'The future of spam litigation after *Omega World Travel v Mummagraphics*' (2007) 20/2 *Harvard Journal of Law & Technology* 459-78

Yang (2004-2005) 4/1 *Chicago-Kent Journal of Intellectual Property*
Yang GC 'CAN-SPAM: A first step to no spam' (2004-2005) 4/1 *Chicago-Kent Journal of Intellectual Property* 1-44

Youngblood (2001) 11/1 *DePaul-LCA Journal of Art and Entertainment Law*
Youngblood C 'A new millennium dilemma: Cookie technology, consumers, and the future of the Internet' (2001) 11/1 *DePaul-LCA Journal of Art and Entertainment Law* 45-82

JUDICIAL DECISIONS

South Africa

Jafta v Ezemvelo KZN Wildlife (2009) 30 ILJ 131 (LC)

Ketler Investment CC Presentations v Internet Service Providers' Association 2014 (1) ALL SA 566 (GSJ)

Sihlali v South African Broadcasting Corporation Ltd [2010] ZALC 1, (2010) 31 ILJ 1477 (LC)

Spring Forest Trading v Wilberry (Pty) Ltd t/a Ecowash Combined Motor Holdings Limited (725/13) [2014] ZASCA 178; 2015 (2) SA 118 (SCA)

Australia

Australian Communications and Media Authority v Atkinson [2009] FCA 1565 (22 December 2009) 1-18 http://www.austlii.edu.au/cases/cth/federal_ct/2009/1565.html (date of use: 15 January 2016)

Australian Communications and Media Authority v Clarity 1 Pty Ltd [2006] FCA 1399 1-18 http://www.austlii.edu.au/au/cases/cth/federal_ct/2006/1399.html (date of use: 15 January 2016)

Australian Communications and Media Authority v Mobilegate Ltd [2010] FCA 1197 (5 November 2010) 1-35 http://www.austlii.edu.au/au/cases/cth/FCA/2010/1197.html (date of use: 15 January 2016)

AustraliaSMS Pty Ltd (ABN 30 100 396 138 and ACN 100 396 138 media release 21 July 2005) 1-7 http://www.acma.gov.au/webwr/assets/main/lib310480/aust/sms-boulos-ast_enforc_utaking.pdf (date of use: 20 January 2016)

Best Buy Australia Pty Ltd (ACN 122 464 799 media release 24 February 2010) 1-8 http://www.acma.gov.au/~/media/Unsolicited%20Communications%20Compliance/enforceable%20understanding/pdf/EU%20Best%20Buy%20Australia%20PL%20Augst%202010%20Spam%20Act%202003.PDF (date of use: 20 January 2016)

Big Mobile Pty Ltd (ACN 119 902 966 media release 29 September 2009) 1-6 http://www.acma.gov.au/webwr/_assets/main/lib310480/big_mobile_s38_spamact.eu.pdf (date of use: 20 January 2016)

Club Retail Pty Ltd (ACN 165 324 881 media release 2015) 1-3 http://www.152.91.62.26/sitecore/content/Home/Citizen/Take-action?Complaints/Spam-complaints/Spam-complaints/spam-enforcement-actions (date of use: 15 January 2016)

DND Media Pty Ltd (ACN 151 096 285 media release 05 September 2013) 1-2 http://www.acma.gov.au/~/media/Unsolicited%20Communications%20Compliance/Formal%20warning/DND%20Media%20s41%20Spam%20Act%20Formal%20Warning%20%20pdf.pdf (date of use: 20 January 2016)

EventsHQ Pty Ltd (ACN 118 063 666 media release 13 January 2012) 1-6 http://www.acma.gov.au/webwr/_assets/main/lib310480/eventshqs38_spamacteu.pdf (date of use: 20 January 2016)

Funmobile Australia Pty Ltd (ACN 114 489 600 media release 19 January 2010) 1-6 http://www.acma.gov.au/webwr/_assets/main/lib310480/funmobiles38spamact.eu.pdf (date of use: 20 January 2016)

Global Billing Solutions Pty Ltd (ACN 135 029 748 media release 23 March 2012) 1-2 http://www.acma.gov.au/webwr/_assets/main/lib410040/global_billing_solutions-formal_warning_spam_act.pdf (date of use: 20 January 2016)

IGEA Life Sciences Pty Limited (ACN 125 930 878 media release 30 June 2014) 1-2 http://www.acma.gov.au/~/media/Unsolicited%20Communications%20Compliance/Formal%20warning/PDF/20140630%20%20IGEA%20Life%20Sciences%20Pty%20Limited%20%20Formal%20warning%20pdf.PDF (date of use: 20 January 2016)

JER Pty Ltd (CAN 107 555 475 19 October 2011) 1-4 http://www.acma.gov.au/webwr/_assets/main/lib310480/urban_agent-eus38spamact.pdf (date of use: 20 January 2016)

McDonald's Australia Limited (ACN 008 496 928 media release 18 December 2012) 1-2 http://www.acma.gov.au/Industry/Marketers/Anti-Spam/ Ensuring-you-don'tspam/mr-992012-acma-warns-mcdonalds-for-send-to-friends-marketing (date of use: 20 January 2016)

New Dialogue Pty Limited (ACN 111 086 938 media release 29 September 2009) 1- http://www.acma.gov.au/webwr/_assets/main/lib310480/new_dialogue_s38_spam_act_eu.pdf (date of use: 20 January 2016)

Nokia Corporation (media release 03 January 2012) 1-6 http://www.acma.gov.au/webwr/assets/main/lib310480/nokia eus38spamact3jan2012.pdf (date of use: 20 January 2016)

Oxygen8 Communications Australia Pty Ltd (ACN 111 902 982 media release 15 December 2008) 1-6 http://www.acma.gov.au/webwr/_assets/main/lib310480 /oxygen8_s38_spam_act.pdf (date of use: 20 January 2016)

Penta Group Pty Ltd (ACN 122757519 media release 2014) 1-2 http://www.acma.gov.au/theACMA/penta-group-pty-ltd (date of use: 20 January 2016)

Qidi Enterprises Pty Ltd (ABN 35097220114 media release 20 January 2006) 1-7 http://www.acma.gov.au/webwr/_assets/main/lib310480/p_liang_qidi_enterprisesast_enforc_utaking.pdf (date of use: 20 January 2016)

Tiger Airways Holdings Limited (ACN 124 369 008 media release 22 October 2012) 1-9 http://www.acma.gov.au/webwr/_assets/main/lib310480/tiger_airways%20eu_s38_spam_act-22oct2012.pdf (date of use: 20 January 2016)

Vadkho Pty Ltd (ACN 138 809 917 media release 22 April 2015) 1-2 http://www.acma.gov.au/Citizen/Take-action/Complaints/Spam-complaints/spam-enforcement-actions (date of use: 20 January 2016)

Virgin Blue Pty Limited (ACN 090 670 965 26 February 2010) 1-8 http://www.acma.gov.au/webwr/_assets/main/lib310480/virgin_blue_s38_spam_actenforceable_undertaking.pdf (date of use: 20 January 2016)

Wailea Australia Pty Ltd (ACN 155 959229 media release 07 October 2013) 1-2 http://www.acma.gov.au/~/media/Unsolicited%20Communications%20Compliance/Formal%20warning/ACRIS%20Svces%20ss161%20Formal%20warning%20Spam%20Act%20pdf.pdf (date of use: 20 January 2016)

United States of America

Balsam v Trancos Inc 2012 WL 593703 (Ca Ct App Feb 24 2012) 1-5 http://blog.ericgoldman.org/archives/2012/02/california_appe_2.htm (date of use: 30 December 2015).

Beyond Systems INC. v Kraft Foods Incorporated (2014 WL 3572771 July 21 2014) 1-13 http://caselaw.findlaw.com/us-4th-circuit/1691263.html (date of use: 30 December 2015).

Beyond Systems Inc v Keynetics Inc 422 F Supp 2nd (2006) 1-60 http://www.steptoe.com/assets/attachments/1923.pdf (date of use: 30 December 2015)

Commonwealth of Virginia v Jeremy Jaynes (No 08-765) 1-31 http://www.scotusblog.com/wp-content/uploads/2009/03/08-765_bio.pdf (date of use: 30 December 2015)

Federal Trade Commission v Lance Thomas Atkins (Case No 08CV5666 2009) 1-25 http://www.ftc.gov/sites/default/files/documents/cases/2009/11/091130atkinsjudgemnt.pdf (date of use: 30 December 2015)

Federal Trade Commission v Phoenix Avatar, LLC trading as Avatar Nutrition (Case No 04C 2897 2004) 1-24 http://www.ftc.gov/sites/default/files/ documents/cases/2005/03/050331stip0423084.pdf (date of use: 30 December 2015)

Federal Trade Commission v Sili Neutraceuticals LLC (Case No 07 C 4541 2008) 1-20 http://www.ftc.gov/sites/default/files/documents/cases/2008/02/080123silidefaultjdgnt.pdf (date of use: 30 December 2015)

Federal Trade Commission v Spear Systems Inc (Case No 07 c 5597 2009) 1-22 http://www.ftc.gov/sites/default/files/documents/cases/2009/07/090702xavierjudgeorder.pdf (date of use: 30 December 2015)

FTC v Global Web Promotions Pty Ltd (Case No 04C 3022 2005) 1-23 http://www.ftc.gov/sites/default/files/documents/cases/2005/09/050920defjudg042386.pdf (date of use: 30 December 2015)

Gordon v Virtumundo 575 F 3d 1040 (2009 *US App LEXIS* 17518) 1-28 http://www.nyls.edu/wp-content/uploads/sites/141/2013/08/575-F.3d-1040-Gordon-v-Virtumundo.pdf (date of use: 30 December 2015)

Kleffman v Vonage Holdings Corp 232 P 3d 625, 627 (Cal 2010) http://www.caselaw.findlaw.com/ca-supreme-court/1527999.html (date of use: 5 January 2016)

Omega World Travel v Mummagraphics 469 F 3d 348 94th Cir 2006 1-9 http://openjurist.org/469/f3d/348/omega-world-travel-incorporated-v-mummagraphics-incorporated-w (date of use: 30 December 2015)

Parker v CN. Enterprises (Case No 97-06273 Texas Travis County District Court November 1997) 1-3 http://www.loudy.com/CASES/Parker_v_CN_Entterprises.html (date of use: 30 December 2015)

Spam Arrest LLC v Replacements Ltd (2013) WL 4675919 (WD Wash. Aug. 29 2013) 1-36 https://cases.justia.com/federal/district-courts/washington/wawdce/2:2012cv00481/182956/96/0.pdf?ts=1377958938http://blog.ericgoldman/archives/2013/09/spamarrests.se.htm (date of use: 30 December 2015)

US v Kilbride 584 F 3d 1240 (9th Cir 2009) 1-19 http://www.nyls.edu/wp content/uploads/sites/141/2013/08/584-F.3d-1240-US-v.-Kilbride.pdf (date of use: 30 December 2015)

US v Twombly 475 F Supp 2nd 1019 (SD Cal 2007) 1-11 https://casetext.com/case/us-v-twombly-2 (date of use: 30 December 2015)

Wagner v Spire Vision (C13-04952 WHA ND Cal March 2014) 1-16 http://blog.ericgoldman.org/archives/2014/06/can-spam-preemption-doesnt-apply-to-fraud-and-more.htm (date of use: 30 December 2015)

White Buffalo Ventures v University of Texas at Austin 420 F 3d 366 (5th Cir 2005) 1-13 http://www.openjurist.org/420/f3d/366/white-buffalo-ventures-llc-v-university-of-texs-at-austin (date of use: 30 December 2015)

LEGISLATION AND FOREIGN LEGAL INSTRUMENTS

SOUTH AFRICA

Acts

Business Names Act 27 of 1960

Consumer Affairs (Unfair Business Practice) Act 71 of 1988

Consumer Protection Act 68 of 2008

Electronic Communications and Transactions Act 25 of 2002

Financial Advisory and Intermediary Services Act 37 2002

Guidelines for Recognition of Industry Representative Bodies of Information System Providers' (IRB Code) GN 1283 *GG* 29474 (14 December 2006)

Merchandise Marks Act 17 of 1941

National Consumer Credit Act 34 of 2005

Price Control Act 25 of 1964

Protection of Personal Information Act 4 of 2013

Sales and Service Matters Act 25 of 1964.

Trade Practices Act 76 of 1976

Bills

Cybercrimes and Cybersecurity: Bill (Draft for Public Comment) *Government Gazette GG* No. 39161 Notice 878 (30 November 2015) http://www.justice.gov.za/legislation/notices/2015/20150902-gg39161_gen878-cyberbill.pdf (date of use: 20 January 2016)
Cybercrimes and Cybersecurity Bill *Government Gazette GG* No. 40487 (9 December 2016) http://ellipsis.co.za/wp-content/uploads/2017/02/b-6-2017-cybercrimes.pdf (date of use: 4 March 2017)

Electronic Communications and Transactions Amendment Bill *Government Gazette GG* No. 35821 Notice 888 (26 October 2012) http://www.ellipsis.co.za/wp-content/uploads/2012/10/Electronic-Communications-and-Transactions-Amendment-Bill-2012-for-public-comments-20121026-GGN-35821-00888.pdf (date of use: 30 November 2015).

Other documents

The Department of Communications *Green Paper on e-Commerce: Making it your business* (2000)

South African Law Reform Commission (SALRC) Discussion Paper 109 Project 124 *Privacy and Data Protection* (2005)

AUSTRALIA

Acts

Spam Act of 2003

Trade Practices Act of 1974

Other documents

ACMA 'Australian eMarketing Code of Practice' (March 2005) 1-67 http://www.acma.gov.au/~/media?Unsolicited%20Communications%20Compliance/Regulation/pdf?Australia%20EMarketing%20Code%20of%20Practice.pdf (date of use: 20 January 2016)
ACMA 'Joint select committee on cyber-safety submission no. 80' (July 2010) 1-28 http://www.aphref.aph.gov.au-house-committee-jscc-subs-sub_80%20(3).pdf (date of use: 20 January 2016)
ACMA 'Regulation guide: no 5 infringement notices' (September 2011) 1-6 http://www.acma.gov.au/~/media/Legal%20Services/Advice/pdf/Regulatory%20guide%20No%205%20Infringement%20notices.PDF (date of use: 15 January 2016)
ACMA 'Submission to Spam Act Review' (Melbourne 2006) 1-30 http://www.acma.gov.au/webwr/consumer_info/spam/acma%20submission%20to%20review.pdf (date of use: 15 January 2016)

Joint Statement between the Department of Communications Information Technology and the Arts (Australia) and the Ministry of Information and Communication Technology of the Kingdom of Thailand Concerning Cooperation in the Fields of Communications and Information Technology 1-2 http://www.acma.gov.za.au (date of use: 20 January 2016)

Memorandum of Understanding between Australia Commerce and Industry Office, and the Taipei Economic and Cultural Office in Australia Concerning Cooperation in the Cooperation in the Regulation of Spam (signed in October 2007) 1-4 http://www.acma.gov.au/~/media/Unsolicited%20Communications%20Compliance/Information/pdf/Spam%20International%20Cooperation%20Memorandum%20of%20Understanding%20Between%20Australia%20and%20%Taiwan.Pdf (date of use: 20 January 2016)

Memorandum of Understanding between the Australian Communications and Media Authority (ACMA) and the New Zealand Department of Internal Affairs (DIA) 1-10 http://www.acma.gov.au/~/media/Unsolicited%20Communications%20Compliance/Information/pdf/Spam%20International%20Cooperation%20Memorandum%20Understanding%20Between%20Australia%20and%20New%20Zealand.PDF (date of use: 20 January 2016)

Memorandum of Understanding between the Korean Information Security Agency and the Australian Communications Authority and the National Office for the Information Economy of Australia Concerning Cooperation in the Regulation of Spam 1-3 http://www.itu.int/osg/spu/spam/contributions/Attachments%20Memorandum%20of%20Understanding%20Between%20KISA%20ACA%20and%20and%20NOIE.pdf (date of use: 20 January 2016)

Memorandum of Understanding on continual enforcement assistance in commercial email matters among the following agencies of the United States; the United Kingdom and Australia: The United States Federal Trade Commission; the United Kingdom's Office of Fair Trading; the United Kingdom's Information Commissioner; Her Majesty's secretary of State for Trade and Industry in the United Kingdom; the Australian Competition and Consumer Commission; and the Australian Communications Authority 1-11 http://www.ftc.gov/sites/default/files/attachments/international-antitrust-and-consumer-protection-cooperation agreements/040630spammoutext.pdf (date of use: 20 January 2016)

Seoul-Melbourne Multilateral Memorandum of Understanding on Cooperation in Countering Spam (signed 4 May 2010) 1-8 http://www.sm-mou.org/smmou/about.mou.php (date of use: 20 January 2016)

Spam Regulations 2004 *Commonwealth of Australia Gazette* (8 April 2004). http://www.austlii.edu.au/au/legis/cht/num_reg_es/sr20042004n56202.html (date of use: 15 January 2016).

CANADA

Acts

Canada Anti-Spam Legislation of 2014

JAPAN

Acts

Law on Regulation of Transmission of Specified Electronic Mail Act passed April 2002, amended in 2005 and 2008 http://www.mofo.com/resources/publications/2008/07/japanese-new-anti_spam.law (date of use: 7 September 2015).

UNITED STATES OF AMERICA

Acts

Alaska Statutes: Title 45 Trade and Commerce; Chapter 50 Competitive Practices and Regulation of Competition; section 479 Limitation of electronic mail (added by 2003 Alaska Laws ch.14, H.B 82 2003, approved May 5 2003 effective July 30 2003)

Arizona Revised Statutes Title 44: Trade and Commerce; Chapter 9. Trade Practices Generally; Article 16. Commercial e-mail (added by 2003 S.B 1280 approved May 16 2003)

Arkansas Code Title 4: Business and Commercial Law; Subtitle 7 Consumer Protection; Chapter 88: Deceptive Trade Practices Subchapter 6: Unsolicited Commercial and Sexually Explicit Electronic Mail Prevention Act (added by Act 1019 of 2003 (approved April 2 2003))

California Business and Professions Code: Division 7; Part 3, Chapter 1: Article 1.8 Restrictions on Unsolicited Commercial E-Mail Advertisement (added by Stats. 2003 ch. 487 (SB 186), approved September 23 2003 as amended).

Connecticut General Statutes: Title 52 Civil Actions; Chapter 925 Statutory Rights of Action and Defenses (as amended in 2003)

Controlling the Assault of Non-Solicited Pornography and Marketing Act (CAN-SPAM Act of 2003)

Communications Act of 1934 (47 USC 231(e)(4)

Delaware Code: Title 11 Crimes and Criminal Procedure (as amended by 72 Del. Laws c 135 approved by Governor June 23, 1999; effective July 2 1999)

Federal Trade Commission Act of 1914 (as amended)

Florida Rules of Professional Conduct (Fla. R.P.C) Rule 4-7.6(c) (3) http://www.law.cornell.edu/ethics/fl/code/FL_CODE.HTM (date of use: 30 December 2015)

Federal Deposit Insurance Act (12 USC 1818)

Florida Rules of Professional Conduct (Fla RPC) rule 4-7.6(c)(3) http://www.law.cornell.edu/ethics/fl/code/FL_CODE.HTM (date of use: 30 December 2015)

Florida Statutes: Title 39 Commercial Relations; Chapter 668 Electronic commerce; part III Federal Credit Union Act (12 USC 1751) e-mail communications

(added by 2004 Fla. Laws ch. 233, approved May 25 2004, effective July 1 2004)

Idaho Code Title 48: Monopolies and Trade Practices; Chapter 6: Consumer Protection Act; section 48-603E. Unfair Bulk Electronic Mail Advertisement Practices (added by House Bill 505 (approved by Governor April 17 2000 (effective July 1 2000))

Illinois Compiled Statutes: Chapter 815 Business Transactions Deceptive Practices; 815 ILCS 511/ Electronic Mail Act

Iowa Code Chapter 714E (added by House File 448 (1999) approved by Governor May 26 1999 (effective July 1 1999))

Kansas Statutes: Chapter 50 Unfair Trade and Consumer Protection; Article 6 Consumer Protection (added by Laws 2002 ch 140 (SB 467) approved May 17 2002)

Kentucky Bar Association Rules of the Supreme Court of Kentucky (Ky Sup Ct) http://www.cle.kybar.org/documents/scr/scr3/scr_3.130_(7.09).pdf (date of use: 5 January 2016)

Louisiana Revised Statutes: Title 14 Criminal Law; (as amended by 1999 La. Acts 1180 approved July 9 1999).

Louisiana Revised Statutes: Title 51 Trade and Commerce Chapter 19-C Unsolicited Commercial E-mail Restrictions (added by 2003 La. Acts 1275, approved July 2 2003)

Maine Revised Statutes Title 10 Commerce and Trade Part 3 Regulation of Trade Chapter 224 e-mail Solicitation (added by Public Laws ch. 327 (2003), H.B. 210 (approved May 27 2003)

Maryland Criminal Law Code Title 3: Other Crimes against the Person; Subtitle 8: Stalking and Harassment (as amended in 2004)

Michigan Compiled Laws Chapter 445. Trade and Commerce Unsolicited Commercial e-mail Protection Act (added by 2003 Mich Pub Act 42 (HB 4519) effective 1 September 2003)

Minnesota Statutes 2002 Ch 395 Senate file no 2908 (2002) (introduced 11 February 2002 approved 20 May 2002)

Missouri Revised Statutes Title 26: Trade and Commerce Chapter 407. Merchandising Practices and Electronic Mail Practices (enacted in 2000) amended by House Bill 228 (2003) approved 11 July 2003 (effective 28 August 2003)

New Mexico Statutes: Title 57 Trade and Commerce Article 12 Unfair Practices Act (added by 2003 SB 699 2003 NM Acts ch 168 approved 5 April 2003)

North Carolina General Statutes (as amended in 1999)

North Dakota Statutes: Title 51 Sales and Exchanges Chapter 27 Commercial E-mail Solicitation (added by session laws 2003 ch 439 (HB 1388)

Official Code of Georgia: Title 16 Crimes and Offences Chapter 9 Forgery and Fraudulent Practices Article 6 Computer Systems Protection (as amended by Senate Bill 62 2005 approved and effective 19 April 2005)

Ohio Revised Code: Title 23 Courts Common Pleas Chapter 2307 Civil Actions Damage and Theft (as amended by HB 361 2005 effective 6 May 2005)
Oklahoma Statutes: Title 15 Contracts (added by Okla. Laws 1999 ch 337 House Bill 1410 1999 (approved by Governor 8 June 1999 effective 1 July 1999 amended by Senate Bill 660 2003 effective 1 November 2003)

Pennsylvania Statutes: Title 73 Trade and Commerce Chapter 40A Unsolicited Telecommunication Advertisement Act (added by 2002 Pa Laws 222 approved 16 December 2002)

Revised Code of Washington: Title 19 Business Regulations-Miscellaneous Chapter 19.190 Commercial Electronic Mail (as amended by 2003 Acts ch 137 (HB 2007))
Rhode Island General Laws Title 6: Commercial Law General Regulatory Provisions Chapter 47 Internet access and Advertising by Facsimile (added in 1999)

South Dakota Codified Laws: Chapter 37-24 Deceptive Trade Practices and Consumer Protection (provisions added or amended in 2002)

Tennessee Code Title 39: Criminal Offences Chapter 14 Offenses against Property: Part 6 Tennessee Personal and Commercial Computer Act of 2003 (added in 2003)
Texas Statutes Title 4: Business & Commerce Code Chapter 46 Electronic Mail Solicitation (added by Acts 2003 ch 1053 (House Bill 1282) approved 20 June 2003 effective 1 September 2003)

Utah Code: Title 13 Commerce and Trade Chapter 36 Unsolicited Commercial and Sexually Explicit E-mail Act (added by Utah Laws 2002 Chapters 125 and 229)

Virginia Code: Title 18.2 Crimes and Offenses Generally Chapter 5 Crimes against Property Article 7.1 Computer Crimes (including amendments by Acts 2003 ch 987 & 1016 approved 3 April 2003)

Wisconsin Statutes: Chapter 944 Crimes against Sexual Morality (added by 2001 Act 16 approved 1 June 2001)
Wyoming Statutes: Title 40 Trade and Commerce Chapter 12 Consumer Protection Article 4 Commercial Electronic Mail (added by 2003 Wyo Laws ch 86 approved 3 March 2003 effective 1 July 2003)

Other documents

Code of Federal Regulation (CFR) Part 316 Title 16 Commercial Practices

Federal Trade Commission 'National do not e-mail registry: a report to congress (2004) the executive summary' https://www.ftc.gov/sites/default/files/documents/reports/can-spam-act-2003-national-do-not-email-registry-federal-trade-commission-report-congress/report.pdf (date of use: 30 December 2015).
Federal Trade Commission 'Online profiling: a report to Congress part 2

recommendations' 1-2 http://www.steptoe.com/assets/attachments/934.pdf (date of use:10 November 2015)

Federal Register 'Requirements to place warning labels on commercial electronic mail that contains sexually oriented material' 69 19 (29 January 2004) http://www.uspto.gov/sites/default/files/web/offices/com/sol/notices/69fr4269.pdf (date of use 6 January 2016)

Memorandum of Understanding on continual enforcement assistance in commercial email matters among the following agencies of the United States; the United Kingdom and Australia: The United States Federal Trade Commission; the United Kingdom's Office of Fair Trading; the United Kingdom's Information Commissioner; Her Majesty's secretary of State for Trade and Industry in the United Kingdom; the Australian Competition and Consumer Commission; and the Australian Communications Authority 1-11 http://www.ftc.gov/sites/default/files/attachments/international-antitrust-and-consumer-protection-sooperation-agreements/050224memounderstanding.pdf (date of use: 30 December 2016)

Memorandum of Understanding between the United States Federal Trade Commission and the Information Commissioners Office of the United Kingdom on Mutual Assistance in the Enforcement of Laws Protecting Personal Information in Private Sector. Document accessed (2014) 1-10 http://www.ftc.gov/systems/files/attachments/international-competition-consumer-protection-cooperstion-agreements/140306ftc-uk-mou.pdf (date of use: 30 December 2015).

Memorandum of Understanding between US FTC and the Federal Republic of Nigeria's Consumer Protection Council (CPC) and Economic and Financial Crimes Commission (EFCC) on Mutual Enforcement Assistance in Consumer Protection Matters (2013) 1-2 http://www.ftc.gov/news-events/press-releases/2013/08/ftc-signs-memorandum-understandu=ing-nigerian-consumer-protection (date of use: 30 December 2015)

Memorandum of Understanding on Mutual Enforcement Assistance in Commercial Email Matters Between the Federal Trade Commission of the United States of America and the Agencia Espanola De Proteccion De Datos 1-9 http://www.ftc.gov/sites/defaults/files/attachments/international-antitrust-and-consumer-protection-cooperation-agreements/050224memounderstanding.pdf (date of use: 30 March 2015)

Memorandum of Understanding on Mutual Enforcement Assistance in Commercial E-mail Matters Among the Following Agencies of the United States, the United Kingdom, and Australia: The United States Federal Trade Commission; The United Kingdom's Office of Fair Trading, the United Kingdom's Information Commissioner, Her Majesty's Secretary of the State for Trade and Industry in the United Kingdom, the Australian Competition and Consumer Commission, and the Australian Communications Authority (2 July 2004) 1-11 http://www.ftc.gov/sites/default/files/attachments/international-antitrust-and-consumer-protection-sooperation-agreements/050224 memounderstanding.pdf (date of use: 30 December 2015)

Platt Majoras D et al 'A CAN-SPAM Informant Reward System: A Report to Congress' (September 2004) 1-74 https://ftc.gov/sites/default/files/documents/reports/can-spam-informant-reward-system-federal-trade-commission-report-congressexpert-reports/040916rewardsysrpt.pdf (date of use: 30 December 2015)

Platt Majoras D *et al* 'Subject line labelling as a weapon against spam: A CAN-SPAM Act Report to Congress' (June 2005) 1-46 https://www.ftc.gov/sites/default/files/documents/reports/subject-line-labeling- weapon-against-spam-can-spam-report-congress/050616canspamrpt.pdf (date of use: 6 January 2016)

INTERNATIONAL INSTRUMENTS, MODEL LAWS AND CONVENTIONS

AFRICA

African Union (AU) Convention on Cyber Security and Personal Data Protection adopted by the 23rd Ordinary Session of the Assembly of the Union (27 June 2014 Malabo) https://ccdcoe.org/sites/default/files/documents/AU-270614-CSConvention.pdf (date of use: 9 December 2015)

COMESA Model Law on Electronic Transactions and Guide to Enactment (2010)

Constitutive Act of the African Union (1999) http://www1.uneca.org/Portals/ngm/Documents/Conventions%20and%20Resolutions/constitution.pdf (date of use: 15 December 2015)

Draft African Union Convention on the Establishment of a Credible Legal Framework for Cybersecurity in Africa, also titled Draft African Union Convention on the Confidence and Security in Cyberspace (Version 01/09/2012) http://au.int/en/cyberlegislation (date of use: 9 December 2015)

Declaration and Treaty of the Southern African Development Community (17 August 1992) http://www.sadc.int/files/8613/5292/8378/Declaration_Treaty-of-SADC.pdf (date of use: 9 December 2015)

Official Gazette of the Common Market for Eastern and Southern Africa (COMESA) 16 (15 October 2011)

Southern African Development Community (SADC) Model Law on Electronic Transactions and Electronic Commerce *Harmonization of ICT Policies in Sub-Saharan African* (2013)

Southern African Development Community (SADC) Model Law on Computer Crime and Cybercrime *Harmonization of ICT Policies in Sub-Saharan African* (2013)

ITU

Convention

ITU 'Collection of the Basic Texts of the International Telecommunication Union Adopted by the Plenipotentiary Conference' (2011 ed) https://www.itu.int/dms_pub/itu-s/opb/conf/S-CONF-PLEN-2015-TOC-HTM-E.htm (date use: 6 November 2015)

Other documents

Bambauer DE et al 'A comparative analysis of spam laws: the quest for a Model Law' (Document CYB/03 Geneva, Switzerland 28 June - 1 July 2005) 1-41 https://www.itu.int/osg/spu/cybersecurity/docs/Background_Paper_Comparative_Analysis_of_Spam_Laws.pdf (date of use: 30 November 2015)

Bueti MC 'ITU Survey on Anti-spam Legislation Worldwide' ITU WSIS Thematic Meeting on Cybersecurity (Document CYB/06 Geneva, Switzerland 28 June 1 July 2005) 1-62 http://www.itu-int/osg/spu/spam/legislation/Background_Paper_ITU_Bueti_Survey.pdf (date of use: 30 November 2015)

ITU 'Multilateral and Bilateral Cooperation to Combat Spam' 1-12 http://www.itu.int/osg/spu/spam/contributions/Background%20Paper_Multilateral%20Bilateral%20Coop.pdf (date of use: 30 November 2016)

ITU-T Series X: Data Networks Open System Communications and Security (Cyberspace security countering spam) 'Framework for countering spam in IP based multimedia applications' (Recommendation ITU-T X.1245 (12/2010) 1-23 http://www.itu.rec/T-REC-X.1245-201012-l/en (date of use: 30 November 2015)

ITU-T Series X: Data Networks Open System Communication and Security (Cyberspace security countering spam) 'Interactive gateway system for countering spam' (Recommendation ITU-T X.1243 (12/2010) 1-22 http://www.itu.int/ITU-T/recommendations/rec.aspx?rec=10829 (date of use: 05 December 2015)

ITU-T Series X: Data Networks Open System Communications and Security 'Supplement on a practical reference model for countering e-mail spam using botnet information' (Series X.1243) 1-16 http://www.itu.int/ITU-T/recommendations/rec.aspx?rec=11755 (date of use: 30 November 2015)

ITU-T Series X: Data Networks Open System Communications and Security ITU-T X 1240 Series 'Supplement on Countering Spam and Associated Threats' (Supplement 6) (09/2009) http://www.itu.int/ITU-T/recommendations/ rec/aspx?rec=10245 (date of use: 30 November 2015)

ITU-T Series X: Data Networks Open System Communications and Security 'Supplement on framework based on real time blocking lists for countering VoIP spam' (ITU-T X.1245 Recommendation: Supplement 11 (09/2011) 1-18 http://www.itu.int/ITU-T/recommendations/rec.aspx?rec=11342 (date of use: 30 November 2015).

ITU-T Series X: Data Networks Open System Communications and Security (Telecommunication security) 'Technical framework for countering email spam' (Recommendation ITU-T X.1241 (04/2008)) 1-11 http://www.itu.int/ITU-T/recommendations/rec.aspx?rec=9335 (date of use: 30 November 2015)

ITU-T Series X: Data Networks Open Systems Communications and Security (Telecommunications security) 'Technical strategies for countering spam' (Recommendation ITU-T X.1231 (04/2008) 1-11 http://www.itu.int/ITU-T/recommendations/rec.aspx?rec=9333 (date of use: 30 November 2015)

ITU-T Series X: Data Networks Open System Communications and Security (Telecommunication security) 'Technologies involved in countering e-mail spam' (Recommendation ITU-T X.1240 (04/2008)) 1-19 http://www.itu.int/ITU-T/recommendations/rec.aspx?rec=9334 (date of use: 30 November 2015)

ITU-T Telecommunication Standardization Sector of ITU World Telecommunication Standardization Assembly (WTSA) 'Resolution 51: Combating Spam' (Resolution passed Florianopolis 5-14 October 2004) 1-3 http://www.itu.int/ITUT/wtsa/resolutions04/Res51E.pdf (date of use: 30 November 2015)

ITU-T World Telecommunication Standardization Sector of ITU World Countering Spam (Resolution passed Florianopolis 5-14 October 2004) 1-3 http://www.itu.int./dms_pub/ITU-T/opb/res/T-RES-T.52-2012-PDF-E.pdf (date of use: 30 November 2015)

ITU-T World Telecommunication Standardization Assembly (WTSA) (resolution was passed in Dubai, 20-29 November 2012) 'Resolution 52: Countering spam' (renamed 'Countering and combating spam' http://www.itu.int./dms_pub/ITU-T/opb/res/T-RES-T.52-2012-PDF-E.pdf (date of use: 30 November 2015).

ITU WCIT 'Final Acts World Conference on International Telecommunications' Dubai 2012) 1-30 http://ww.itu.int/en/ITU-T/Workshops-and-Seminars/spam/201307/pages/default.aspx (date of use: 30 November 2015)

ITU WSIS Thematic Meeting on countering spam curbing spam via technical measures: an overview 1-18 http://www.itu.int/osg/spu/spam/contributions/Background%20Papercurbing%20Spam%20Via%20Technical%20Measures.pdf (date of use: 30 November 2015)

ITU WSIS Thematic meeting on countering spam 'Multilateral and bilateral cooperation to combat spam' 1-12 http://www.itu.int/osg/spu/spam/contributions/Background%20Paper_Multilateral%2Bilateral%20Coop.pdf (date of use: 30 November 2015)

ITU WSIS Thematic meeting on cyber-security 'A comparative analysis of spam laws: The quest for a Model Law' (Document CYB/03 10 June 2005)

ITU WSIS Thematic workshop on countering spam 'Discussion paper countering spam: How to craft an effective anti-spam law' 1-15 http://www.itu.int/osg/spu/spam/contributions/Background%20Paper_How%20to%2craft%20-effective%20anti-spam%20law.pdf (date of use: 30 November 2015)

Rotenberg M 'Consumer perspectives on spam: challenges and challenges' (2004) 1-19 http://www.itu.int/osg/spu/spam/contributions/Background%20Paper%20consumer%20perspective%20on%20spam.pdf (date of use: 30 November 2015)

Sarrocco C 'Spam the Information Society: Building Frameworks for International Cooperation' 1-28 (2004) http://www.itu.int/osg/spu/spam/contributions/Background%20Paper_Building%20Frameworks%20for%20Int/%20Cooperation.pdf (date of use: 30 November 2015)

OECD

Organisation for Economic Co-operation and Development (OECD) *Task Force on Spam: Anti-Spam-Law Enforcement Report* DSTI/CP/ICCP/SPAM (2004) 3 FINAL (13 May 2005)

OECD 'Report on the OECD Task Force on Spam: Anti-spam ToolKit of Recommended Policies and Measures' (19 April 2006) DSTI/ICCP/SPAM(2005)3/FINAL 1-115 http://www.oecd.org/internet/consumer/36494147.pdf (date of use: 30 November 2015)

UNITED NATIONS

United Nations Conference on Trade and Development (UNCTAD) 'Harmonization of Cyberlaws and Regulation: The Experience of the East African Community (Reforming Cyberlaws Part 1)' UNCTAD/DTL/STICT/2012/4/Corr.1 1-66 http://unctad.org/en/PublicationsLibrary/dtlstict2012d4_en.pdf (date of use: 9 December 2015)

United Nations Commission on International Trade Law (UNCITRAL) Model Law on Electronic Commerce with Guide to Enactment 1996 (with additional article 5 *bis* as adopted in 1998)

United Nations Convention on the Use of Electronic Communications in International Contracts (UNECIC) (2007)

UNCITRAL Model Law on Electronic Signatures with Guide to Enactment (2001)

INTERNET SOURCES

ABSA 'Phishing scams' http://www.absa.co.za/Absacoza/Security-Centre/Scams/Phishing-Scams (date of use: 6 November 2015)

Abbreviations 'What does Whatsapp stand for?' http://www.abbreviations.com/whatsapp (Date of use: 6 November 2015)

Accessnow 'Africa moves towards a common cybersecurity legal framework' http://www.acessnow.org/blog/2014/06/02/africa-moves-toward-a-common-cyber-security-legal-framework (date of use: 9 December 2015)

Accessnow 'Emerging threats in cybersecurity and data protection legislation in African Union countries' https://www.accessnow.org/emerging-threats-in-cybersecurity-data-protection-in-african-union (date of use: 27 December 2015)

ACMA 'ACMA fights malware at two fronts' http://www.acma.gov.au/Industry/Internet/e-Security/Australian-Intenet-Security-Initiative/acma-fights-malware-on-two-fronts (date of use: 20 January 2016)

ACMA 'ACMA obtains interlocutory orders in SMS spam case' http://www.acma.gov.au/theACMA/acma-obtains-interlocutory-orders-in-sms-spam-case (date of use: January 2016)

ACMA 'Australian eMarketing code of practice' http://acma.gov.au/Industry/Marketers/Anti-Spam/Ensuring-you-dont-spam/australia-emarketing-code-of-practice-ensuring-you-dont-spam-i-acma (date of use: 15 January 2016)

ACMA 'Cellarmaster Wines penalised' (media release May 2013) http://www.acma.gov.au/Industry/Marketers/Anti-Spam/Ensuring-you-dont-spam/cellarmaster-wines-penalised-for-spam-act-breaches (date of use: 20 January 2016).

ACMA 'Do not call register' https://www.donotcall.gov.au (date of use: 20 January 2016)

ACMA 'Double opt-in helps marketers' double check' http://www.acma.gov.au/Industry/Marketers/Anti-Spam/Ensuring-you-dont-spam/double-opt-in-helps-marketers-double-check-1 (date of use: 20 January 2016)

ACMA 'Enforceable undertakings: guidelines for the use of enforceable (Telecommunication Obligations)' March 2006 http://www.acma.gov.au/~/media/Legal%20Services/Advice/pdf/Enforceable%20undertakings%20Guidelines%20Guidelines%20for%20the%20use%20of%20enforceable%20undertakings%20Telecommunications%20Obligations.pdf (date of use: 15 January 2016)

ACMA 'Enforcement action archives' http://www.acma.gov.au/theACMA/acma-enforcement-action-archives (date of use: 15 January 2016)

ACMA 'Federal Court finds Brisbane man breached Spam Act' (December 2010) http://www.acma.gov.au/theACMA/federal-court-finds-brisbane-man-breached-spam-act (date of use: 15 January 2016)

ACMA 'Fighting spam in Australia' http://www.acma.gov.au/theACMA/About/The-ACMA-story/Meeting-our-standard/fighting-spam-in-australia (date of use: 15 January 2016)

ACMA 'Formal warning index' http://www.acma.gov.au/theACMA/formal-warnings
(date of use: 20 January 2016)

ACMA 'Get smart about purchasing lists' http://www.acma.gov.au/theACMA/engage-blogs/engage-blogs/Emarketing/Get-smart-about-purchased-lists (date of use: 15 January 2016)

ACMA 'Inferred consent and conspicuous publications' http://www.acma.gov.au/theACMA/spam-inferred-consent-and-conspicuouspublications (date of use: 20 January 2015)

ACMA 'Introduction to the ACMA' http://acma.gov.au/theACMA/About/Corporate/Authority/introduction-to-the-acma (date of use: 23 March 2017)

ACMA 'Meeting the ACMA standard: fighting spam in Australia' http://acma.gov.au/theACMA/About/The-ACMA-story/Meeting-our-standard/fighting-spam-in-australia (date of use: 15 January 2016)

ACMA 'Million dollar penalties issued in first SMS spam case' http://www.acma.gov.au/theACMA/acma-media-release-1512009-october-million-dollar-penalties-issued-in-first-sms-spam-case (date of use: 15 January 2016)

ACMA ‘Optus penalty for alleged breaches of Spam Act’ (media release January 2009) http://www.acma.gov.au/theACMA/acma-media-release-52009-14-january-optus-pays-penalty-for-alleged-breaches-of-spam-act (date of use: 15 January 2015)

ACMA ‘Penalties awarded in e-mail spam case’ http://www.acma.gov.au/theACMA/acma-media-release-18720009-22december-penalties-awarded-in-email-spam-case (date of use: 15 January 2016)

ACMA ‘Proposed de-registration of spam code’ http://www.acma.gov.au/theACMA/Consultations/Current/proposed-deregistration-of-spam-code (date of use: 20 January 2016)

ACMA ‘Regulatory guides and guidelines’ http://www.acma.gov.au/theACMA/About/The-ACMA-story/Regulating/regulatory-guides-guidelines-limitations-on-control-acma (date of use: 20 January 2016)

ACMA ‘Report spam’ http://www.acma.gov.au/Citizen/Stay-protected/My-online-world/Spamreporting-spam-i-acma (date of use: 20 January 2016)

ACMA ‘Sender identification’ http://www.acma.gov.au/Industry/Marketers/Anti-Spam/Ensuring-you-dont-spam/sender-identification-ensuring-you-dont-spam-i-acma (date of use: 15 January 2016)

ACMA ‘Spam address; harvesting and cold-calling prohibition’ http://www.acma.gov.au/theACMA/spam-address-harvesting-and-cold-calling-prohibition (date of use: 15 January 2016)

ACMA ‘Spam and legislation enforcement’ http://www.acma.gov.au/Industry/Marketers/Anti-Spam/Ensuring-you-dont-spam/spam-legislation-enforcement-ensuring-you-dont-spam-i-acma (date of use: 23 March 2017).

ACMA ‘Spam case studies’ http://www.acma.gov.au/theACMA/spam-case-studies (date of use: 20 January 2016)

ACMA ‘Spam code of practice’ http://www.acma.gov.au/theACMA/Library/Industry-library/Marketers/spam-code-of-practice (date of use: 20 January 2016)

ACMA ‘Spam consent’ http://www.acma.gov.au/Industry/marketers/Anti-Spam/Ensuring-you-dont-spam/spam-consent-ensuring-you-dont-spam-i-acma (date of use: 15 January 2016)

ACMA ‘Spam SMS boosts the ACMA’s fight against spam’ http://www.acma.gov.au/theACMA/acma-media-release-692010-9-june-spam-sms-boosts-the-acmas-fight-against-spam (date of use: 20 January 2016)

ACMA ‘Spam statistics: January 2015’ http://www.acma.gov.au/theACMA/ACMAi/investigation-reports/Statistics/spam-statistics (date of use: 15 January 2016)

ACMA ‘Spam statistics: January 2016’ http://www.acma.gov.au/theACMA/ACMAi/investigation-reports/Statistics/spam-statistics (date of use: 15 January 2016)

ACMA 'Submission to Spam Act Review: ACMA' 5 http://www.acma.gov.au/webwr/consumer_info/spam/acma%20submission%20to%20review.pdf (date of use: 15 January 2016)

ACMA 'The ACMA accepts enforceable undertaking from Alex Shehata' http://www.acma.gov.au/theACMA/the-acma-accepts-enforceable-undertaking-from-alex-shehata (date of use: 20 January 2016)

ACMA 'The ACMA's enforceable undertakings' http://www.acma.gov.au/theACMA/About/The-ACMA-story/Regulating/the-acmas-enforceable-undertakings (date of use: 20 January 2016)

ADMA Do not mail-consumers' https://www.adma.com/au/do-not-mail (date of use: 20 January 2016).

ADMA 'Members Hub' https://www.adma.com.au/members-hub/overview/ (date of use: 20 January 2016)

African Union 'AU in a nutshell' http://www.au.int/en/about/nutshell (Date of use: 9 December 2015)

African Union 'Intergovernmental Authority for Development (IGAD) http://www.au.int/en/recs/igad (date of use: 9 December 2015)

African Union 'History' http://www.au.int/en/about/history (date of use: 9 December 2015)

African Union: INFOSOC 'Cyber Security' http://pages.au/int/infosoc/cybersecurity (date of use: 9 December 2015)

African Union 'Oliver Tambo Declaration' *Extra-Ordinary Conference of African Union Ministers in Charge of Communication and Information Technologies* Johannesburg, South Africa (2-5 November 2009) 1-5 http://www.ernwaca.org/panaf/spip.php?article1154 (date of use: 9 December 2015)

African Union Summit 'Transition from the OAU to the African Union' http://www.au2002.gov.za/docs/background/oau_to_au.htm (date of use: 3 March 2017)

Alfreds D 'Spam declines, malware jumps: Kaspersky' http://www.news24.com/Technology/News/Spam-declines-malware-jumps-Kaspersky-20131119 (date of use: 6 November 2015)

American Cancer Society 'Rumors, myths and truths' http://www.cancer.org/AboutUs/HowweHelpYou/rumours-myths-and-truths (date of use: 5 November 2015)

APEC 'What is Asia-Pacific Economic Cooperation?' http://www.apec.org/About-Us/About-APEC.aspx (date of use: 20 January 2016)

AtomPark Software 'How to gather email addresses and create mailing lists http://www.massmailsoftware.com/ezine/past/2003-03-05.htm (date of use: 10 November 2015).

ATU 'ATU member states as at 25th April 2013' http://www.atu-uat.org/index.php/members/member-states (date of use: 9 December 2015)

ATU 'Goals Strategies' http://www.atu-uat.org/index.php/about-us/core-activity-programmes/global-decision-making (date of use: 9 December 2015)

ATU 'History' http://www.atu-uat.org/index.php/about-us/history (Date of use: 9 December 2015)

AU 'Southern African Development Community (SADC)' http://www.au.int/en/recs/sadc (Date of use: 09 December 2015)

Australian eMarketing code signatory 'Application for signatory status under the Australian eMarketing Code of Practice' http://acma.gov.au/~/media/Unsolicited%20Communications%20Compliance/Form/pdf/Australian%20EMarketing%20Code%20of%20Practice%20Application%20for%20Signatory%20Status.pdf (date of use: 20 January 2016)

Australian Government 'More malware, adware, spyware, spam and spim' http://aic.gov.au/media_library/publications/htcb/htcb011.pdf (date of use: 20 January 2016)

Australian Government Department of Communications Information Technology and the Arts 'Spam Act 2003: A practical guide for government' http://www.acma.gov.au/webwr/consumer_info/spam/spam_act_pracguide_govt.pdf (date of use: 15 January 2015)

Australian Transaction Reports and Analysis Centre 'Penalty units' http://www.austrac.gov.au/enforcement-action/penalty-units (date of use: 15 January)

AVTest 'Spam' https://www.av-test.org/en/statistics/spam (date of use: 07 September 2015)

Bender MR 'Australia's spam legislation: A Modern-Day King Canute' (2006) 1-24 https://papers.ssrn.com/sol3/papers.cfm?abstract_id=916724 (date of use: 15 January 2016)

Bizcommunity 'Telemarketing rings true in South Africa' http://www.bizcommunity.com/Article/196/14/118519.html (date of use: 5 November 2015)

Bonar A 'Buying e-mail lists cheaper than e-mail list rental' http://emailexpert.org/buying-email-lists-cheaper-than-email-list-rental/ (date of use: 10 November 2015)

Bujra A 'Africa: The transition from OAU to AU' Lecture delivered at ACARTSOD Tripoli, Libya http://www.dpmf.org/meetings/From-OAU-AU.html (date of use: 9 December 2015)

BusinessDictionary.com 'Database management system (DBMS)' http://www.businessdictionary.com/definition/database-management-system-DBMS.html (date of use: 5 November 2015)

BusinessDictionary.com 'Personal information' http://www.businessdictionary.com/definition/personal-information.html (date of use: 10 November 2015)

Canadian Radio-television and Telecommunications Commission 'Canada's Anti-spam Legislation' http://crtc.gc.ca/eng/internet/anti.htm (date of use: 7 September 2015)

Chang R 'Could spam kill off e-mail?' (Oct 22 2003) http://www.pcworld.com/article/113061/could_spam_kill_off_e-mail.html (date of use: 10 November 2015)

Chigona W; Bheejun A; Spath M; Derakhashani S and Van Belle JP 'Perceptions on spam in a South African context' *Internet and Information Technology in Modern Organisations: Challenges and Answers* 283-291 http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.515.745&rep=rep1&type=pdf (date of use: 20 January 2016)

Clayton R 'Good practice for combating unsolicited bulk e-mail' http://www.ripe.net/ripe/docs/ripe-206 (date of use: 30 December 2015)

CAUCE 'About CAUCE' http://www.cauce.org/about.html (date of use: 30 November 2015)

CAUCE 'Home' http://www.cauce.org (date of use: 30 November 2015)

CAUCE 'Spam reporting centers' http://www.cauce.org/spam-reporting-centres.html (date of use: 30 November 2015)

Centre for Constitutional Rights and the Electronic Frontier Foundation http://www.elipsis.co.za/cybercrimes-and-cybersecurity-bill (date of use: 20 January)

Cloudmark 'Spammers target mobile users with more than 350,000 unique SMS spam variants in 2012' http://www.cloudmark.com/en/press/spammers-target-mobile-users-with-more-than-350-000-unique-sms-spam-variants-in-2012 (date of use: 6 November 2015)

Coalition against Unsolicited Bulk E-mail, Australia (CAUBE.AU) 'The Problem' http://www.caube.org.au/problem.htm (date of use: 10 November 2015)

COMESA 'About COMESA' http://about.comesa.int/index.php?option=com_content&view=Article&id=75&Itemid=106 (date of use: 9 December 2015)

COMESA 'COMESA member states' http://about.comesa.int/index.php?option=com_content&view=article&id=123&Itemi=121 (date of use: 9 December 2015)

COMESA 'Looking back: evolution of PTA/COMESA' http://about.comesa.int/index.php?option=com_content&view=article&id=95&Itemid117 (date of use: 9 December 2015)

Consumer Affairs 'Feds nab two big spammers: defendants have sent millions of deceptive messages, investigators say http://www.consumeraffairs.com/news04/can_spam.html (date of use: 30 December 2015)

Corbett J 'Reserve Bank launches anti-pyramid scheme campaign' http://www.moneyweb.co.za/reserve-bank-launches-antipyramid-scheme-campaign (Date of use: 6 November 2015)

Cornell University Law School '18 U.S s 1037 – Fraud and related activity in connection with electronic mail' https://www.law.cornell.edu/uscode/text/18/1037 (date of use: 30 December 2015)

Council of Europe Convention on Cybercrime CETS No 185 (23/11/2001 Budapest) http://conventions.coe.int/Treaty/en/Treaties/Html/185.Htm (date of use: 9 December 2015)

Daniels J 'Bulk e-mail or opt-in' http://www.icontact.com/static/pdf/Bulk-E-mail.pdf (date of use: 30 December 2015)

Department of Internal Affairs 'Unsolicited Electronic Messages Act 2007: Prohibiting Spam and Promoting Good Business Practice' http://blog.ubiquity.co.nz/wp-content/uploads/Business-Guide-to-the-Unsolicitedelectronic-Messages-act-2007.pdf (date of use: 20 January 2016)

Department of International Relations and Cooperation (RSA) 'Organization of

African Unity (OAU)/ African Union (AU)' http://www.dfa.gov.za/foreign/Multilateral/africa/oau.htm (date of use: 09 December 2015)

Department of International Relations and Cooperation (RSA) 'Regional Economic Communities (RECs)' http://www.dfa.gov.za/au.nepad/recs.htm (Date of use: 9 December 2015)

Dictionary.com 'Email or e-mail, e-mail' http://dictionary.reference.com/browse/e-mail (date of use: 5 November 2015)

Dictionary.com 'First Amendment' http://www.dictionary.reference.com/browse/first-amendment (date of use: 30 December 2015)

Dictionary.com 'Mouse droppings' http://dictionary.reference.com/browse/mouse+droppings (date of use: 10 November 2015)

Dictionary.com 'Petition' http://www.dictionary.reference.com/browse/petition (date of use: 6 November 2015)

Dictionary.com 'Shareware' http://dictionary.reference.com/browse/shareware (date of use: 10 November 2015)

Dictionary.com 'Trojan horse' http://dictionary.reference.com/browse/trojan+horse (date of use: 10 November 2015)

Dictionary.com 'Web crawler' http://dictionary.reference.com/browse/webcrawler (date of use: 10 November 2015)

Direct Marketing Associating of SA 'The DMA National OPT OUT Database' https://www.nationaloptout.co.za (Date of use: 28 January 2016)

Dube M 'Traditional and emerging partners' role in African Regional Economic Integration: issues and recommendations' *SAIIA* Occasional Paper No 158 Economic Diplomacy Project 1-34 http://dspace.africaportal.org/jspui/bitstream/123456789/1/saia_sop_158 %20_dube_20131204 (date of use: 30 January 2016)

Duermyer R 'Direct mail defined' http://homebusiness.about.com/od/homebusinessglossar1/g/direct_mail_def.htm (date of use: 5 November 2015)

Ellipsis Regulatory Solutions 'The cybercrime and cybersecurity Bill' http://www.elipsis.co.za/cybercrimes-and-cybersecurity-bill (date of use: 28 January 2016)

Emery D 'What is a chain letter?' http://urbanlegends.about.com/od/internet/f/chain_letter.htm (date of use: 5 November 2015)

Encyclopedia of the Unusual and Unexplained 'Superstitions, strange customs, taboos, and urban legends' http://www.unexplainedstuff.com/Superstitions-Strange-Customs-Taboos-and-Urban-Legends/index.html (date of use: 5 November 2015)

European Union 'The history of the European Union' http://www.europa.eu/about eu/eu-history/index_en.htm (date of use: 20 January 2016)

Everett-Church R 'Why spam is a problem' http://www.isoc.org/oti/articles/0599/everett.html (date of use: 7 September 2015)

Federal Trade Commission 'Court orders Australian-based leader of international spam-network to pay $15.15 million: U.S. co-defendant forfeits more than $800.000 and faces jail time' http://www.ftc.gov/news-events/press-releases/2009/11/courtorders-australian-based-leader-international-spam-network (date of use: 15 January 2016)

Federal Trade Commission 'FTC announces first CAN-SPAM cases: two operations generated nearly one million complaints to agency' http://www.ftc.gov/newsevents/press-releases/2004/04/ftc-announces-first-can-spam-act-cases (date of use: 30 December 2015)

Federal Trade Commission 'FTC signs memorandum of understanding with the Mexican consumer protection body' http://www.ftc.gov/news-events/press releases/2005/01/ftc-signs-memorandum-understanding-mexican-consumer-protection (date of use: 30 December 2015)

Federal Trade Commission 'Judge agrees with FTC, orders spammers to pay more than $2.5 million and stop selling bogus weight-loss and anti-aging products' http://www.ftc.gov/news-events/press-releases/2008/02/judge-agrees-ftc-ordersspammers-pay-mpre-25-million-and-stop (date of use: 30 December 2015)

Federal Trade Commission 'Online profiling: a report to Congress part 2 recommendations' http://www.steptoe.com/assets/attachments/934.pdf (date of use: 10 November 2015).

Fidler M & Madzingira F 'The African Union Cybersecurity Convention: a missed human rights opportunity' http://blogs.cfr.org/cyber/2015/06/22/the-african-union-cybersecurity-convention-a-missed-human-rights-opportunity/ (date of use: 27 December 2015)

FindLaw Australia 'Government Spam Act closes down major spammers' http://www.findlaw.com.au/news/4662/government-spam-act-closes-down-majorspammers.aspx (date of use: 15 January 2016)

Finnan D 'Africa: Lack of laws governing cybercrime making Africa a safe haven for Cybercriminals' http://allafrica.com/stories/201502161962.html (date of use: 27 December 2015)

Fletcher D Time 'A brief history of spam' https://content.time.com/time/business/article/0,8599,1933796,00.html (date of use: 10 November 2015)

France24 '1960: The year of independence' http://www.france24.com/en/20100214 1960-year-independence (date of use: 27 December 2015)

FreeAdvice 'What are class A, B, and C misdemeanors' http://criminal.law.freeadvice.com/criminal-law/white_collar_crimes/criminal-misdemeanorclases.html (Date of use: 30 December 2015)

Free Dictionary 'Information age' http://www.thefreedictionary.com/information+age (date of use: 7 September 2015)

Free Dictionary 'Information superhighway' http://www.thefreedictionary.com/information+superhighway (date of use: 7 September 2015)

FTC Consumer Alert 'E-mail address harvesting: how spammers reap what you sow' (November 2002 http://www.webmaestro.biz/pdf/addressharvesting.pdf (date of use: 30 December 2015)

Fuqua J 'Why Lawyers have a bad name: a net legend' http://www.jamesfuqua.com/lawyers/jokers/canter.shtml (date of use: 6 November 2015)

Garfinkel S 'Spam King' https://www.wired.com/1996/02/spam-king (date of use: 6 November 2015).

Githaiga G A Report of the online debate on African Union Convention on Cybersecurity (AUCC)' 1-23 http://www.iitpsa.org.za/wp-content/uploads/2014/02/REPORT-ON-OF-THE-ONLINE-DEBATE-ON-AFRICA-UNION-CONVENTION-ON-CYBERSECURITY.pdf (date of use: 27 December 2015)

Glasner J 'A brief history of spam and spam' http://www.wired.com/2001/05/a-brief-history-of-spam-and-spam (date of use: 5 November 2015)

Goldman E 'Anti-spam lawsuits rarely win, as highlighted by a recent loss by spam arrest' http://www.forbes.com/sites/ericgoldman/2013/09/12/anti-spam-lawsuits-rarely-win-as-highlighted-by-a-recent-loss-by-spam-arrest/ (date of use: 30 December 2015)

GoPetition 'Petitions at GoPetition' http://www.gopetition.com/petitions (date of use: 6 November 2015)

Harris D 'Drowning in sewage spam, the curse of the new millennium: an overview and white paper' http://www.spamhelp.org/articles/drowning-in-sewage.pdf (date of use: 30 December 2015)

HighBeam Research 'ACMA noose chokes off local spam' http://www.highbeam.com/doc/1G1-138418361.html (date of use: 20 January 2016)

Hoax Busters 'The big list of Internet hoaxes' http://www.hoaxbusters.org/#C (date of use: 5 November 2015)

Hoax-Slayer 'Bad advice messages: misleading recommendations' http://www.hoax-slayer.com/bad-advice-emails.html (date of use: 5 November 2015)

Hoax-Slayer 'Sick baby hoaxes-charity hoaxes' http://www.hoax-slayer.com/charity-hoaxes.html for the stories behind these hoaxes (date of use: 5 November 2015)

Hoax-Slayer 'Why do people create e-mail hoaxes' http://www.hoax-slayer.com/why-hoaxes.html (date of use: 5 November 2015)

Hoffman P 'Unsolicited bulk e-mail: definitions and problems' http://www.imc.org/ube-def.html (date of use: 10 November 2015)

Holmes N 'In defence of spam' (2005) 38 *The Profession* 86-8 http://www.eprints.utas.edu.au/1296/1/Cm5Ap0.pdf (date of use: 30 January 2016)

Hormel Foods 'Brand overview' http://www.hormelfoods.com/brands/spam (date of use: 5 November 2015)

Howe W 'Sympathy hoaxes and warm fuzzy stories' http://www.walthowe.com/navnet/legends/sympathylegends.html (date of use: 5 November 2015)

Htxt.africa 'Why the draft cybercrimes Bill should concern South Africans' http://www.htxt.co.za/2015/09/14/why-the-draft-cybercrimes-bill-should-concern-south-africans/ (date of use: 28 January 2016)

ICPEN 'London Plan of Action' http://icpen.org/for-consumer-experts/consumer protection-around-the-world/london-action-plan (date of use: 30 December 2015)

Idea Engineer 'Ask before you send marketing e-mail' http://www.biz-community.com/Article.aspx?c=16&1=196&ai=2969 (date of use: 7 September 2015)

Infoplease 'African Union' http://www.infoplease.com/encyclopedia/history/african-union.html (date of use: 3 March 2017)

Internet Marketing Newswatch 'ACMA launches SpamMatters' http://www.imnewswatch.com/2006/05/30/acma-launches-spammatters (date of use: 20 January 2016)

Internet Service Providers' Association 'Draft cybercrimes and cybersecurity Bill 2015' http://www.ispa.org.za (date of use: 28 January 2016)

Internet Society 'A ten year tribute to Jon Postel' http://www.isoc.org/awards/postel/memory.shtml (date of use: 5 November 2015)

Internet Society 'Brief history of the Internet' http://www.internetsociety.org/internet/what-internet/history-internet/brief-history-internet (date of use: 5 November 2015)

Internet Society Program for joint ATU and the Internet Society seminar on combating spam (9 September 2013 Nairobi Kenya) http://www.internetsociety.org/sites/default/files/ATU%20Spam%20Agenda%20an%20Speakers.pdf (date of use: 9 December 2015)

Investopedia 'Definition of direct marketing' http://www.investopedia.com/terms/d/direct-marketing.asp (date of use: 5 November 2015)

Investopedia 'Definition of telemarketing' http://www.investopedia.com/terms/t/telemarketing.asp (date of use: 5 November 2015)

Investopedia 'Mobile commerce' http://www.investopedia.com/terms/m/mobile-commerce.asp (date of use: 5 November 2015)

Investopedia 'Ponzi scheme' http://www.investopedia.com/terms/p/ponzischeme.asp (date of use: 6 November 2015)

Investopedia 'What is a pyramid scheme' http://www.investopedia.com/articles/04/042104.asp (date of use: 6 November 2015)

IOL News 'Crime: separating the fact from fiction' http://www.iol.co.za/news/south-africa/crime-seperating-the-fact-from-fiction-1.411773#.VlMSl3YrJhE (date of use: 6 November 2015)

ISPA 'About ISPA' http://www.ispa.org.za/about-ispa (date of use: 30 January 2016).

ISPA 'Code of conduct' http://ispa.org.za/code-of-conduct (date of use: 30 January 2016).

ISPA 'ISPA hall of shame' http://ispa.org.za/spam/hall-of-shame/ (date of use: 20 January 2016)

IT Security 'The 25 most mistakes in email security' http://www.itsecurity.com/features/25-common-email-security-mistakes-022807 (date of use: 10 November 2015)

ITU 'About ITU' http://www.itu.int/en/about/Pages?default.aspx (date of use: 30 November 2015)

ITU 'About the ITU-D and the BDT' http://www.itu.int/en/ITU-D/Pages/About.aspx (date of use: 30 November 2015)

ITU 'Council 2005: Note by the Secretary-General Report on spam' Document C05/EP/10-E (Geneva 12-22 July 2005) 2 http://www.itu.int/osg/spu/spam/itu-spam-council-report.pdf (date of use: 30 November 2015)

ITU 'Discover ITU's History' http://www.itu.int/en/History/Pages/DiscoveerITUsHistory.aspx (date of use: 30 November 2015)

ITU 'HIPSSA project: Support for harmonization of the ICT policies in Sub-Saharan Africa' http://www.itu.int/en/ITU-D/Projects/ITU-EC-ACP/HIPSSA/Pages/default.aspx (date of use: 20 March 2017)

ITU 'Legislation and enforcement: a cross-border issue' https://www.itu.int/osg/spu/spam/law.html (date of use: 30 November 2015)

ITU 'ITU and Internet Society collaborate to combat spam" http://www.itu.int/net/pressoffice/press_releases/2014.aspx#.VIvi-E1DGpo (date of use: 7 September 2015)

ITU 'ITU-T in brief' http://www.itu.int/en/ITU-T/about/Pages/default.aspx (date of
use: 30 November 2015)

ITU 'ITU-T study groups (study period 2013-2016)' http://www.itu.int/en/ITU T/studygroups/2013-2016/Pages/default.aspx (date of use: 30 November 2015)

ITU 'ITU-T study group 10 (study period 2001-2004)' http://www.itu.int/ITU T/studygroups/com10/index.html (date of use: 30 November 2015)

ITU 'ITU-T study group 17 (study period 2005-2008)' http://www.itu.int/ITU-T/2005- 2008/com17/tel-security.html (date of use: 30 November 2015)

ITU 'ITU-T work programme' http://www.itu.int/itut/ workprog/wpblock.aspx?isn=1759 (date of use: 30 November 2015)

ITU 'Merger of study groups 7 and 10 into new study group 17' http://www.itu.int/ITU-T/studygoups/com07/merger.html (date of use: 30 November 2015)

ITU 'Short history of study group 17' http://www.itu.int/en/ITU-T/studygroups/2013 2016/17/Pages/history.aspx. (date of use: 30 November 2015)

ITU 'Study group 17 at a glance' http://www.itu.int/en/ITU T/about/groups/Pages/sg17.aspx (date of use: 30 November 2015)

ITU 'The framework of ITU-T' http://www.itu.int/en/ITU T/about/Pages/framework.aspx (date of use: 30 November 2015)

ITU 'Virtual Conference on Regulatory Cooperation on Spam' http://www.itu.int/ITU-D/treg/Events/semonars/Virtual-events/Spam/index.html (date of use: 30 November 2015)

ITU 'What does ITU do?' http://www.itu.int/en/about/Pages/whatwedo.aspx (date of use: 30 November 2015)

ITU 'Workshop on countering and combating spam' (Durban South Africa 8 July 2013) http://www.itu.int/en/ITU-T/Workshops-and Seminars/spam/201307/Pages/default.aspx (date of use: 30 November 2015)

ITU World Summit on the Information Society 'First phase Geneva (10-12 December 2015) the Summit' http://www.itu.int/wsis/geneva/index.html (date of use: 30 November 2015)

ITU 'WSIS Thematic Meeting on Countering Spam: Chairman's Report' http://www.itu.int/osg/spu/spam/chairman-report.pdf (date of use: 30 November 2015)

ITU World Summit on the Information Society 'Plan of Action' Document WSIS 03/GENEVA/DOC/5-E (12 December 2003) http://www.itu.int/net/wsis/docs/geneva/official/poa.html (date of use: 30 November 2015)

ITU World Summit on the Information Society (WSIS) 'Thematic Meeting on Countering Spam' (Geneva, 07-09 July 2004) http://www.itu.int/osg/spu/spam/presentations/HORTON-OpeningRemarks.pdf (date of use: 30 November 2015)

ITU WSIS 'WSIS+10 High Level Event' (Geneva 10-13 June 2014) http://www.itu.int/net/wsis/implementation/2014/forum (date of use: 5 November 2015)

ITU-T 'Africa united in combatting spam and e-waste' http://www.itu.int/en/ITU T/Workshop-and-Seminars/spam/201307/Pages/Default.aspx (date of use: 9 December 2015)

ITU-T 'Study Group 7 area of responsibility (study period 1997-2000)' http://www.itu.int/ITU-T/1997-2000/com07/area-resp-old.html (date of use: 30 November 2015)

ITU-T 'Study groups (study period 2013-2017)' http://www.itu.int/en/ITU T/studygroups/2013-2016/17/Pages/countering -spam.aspx (date of use: 30 November 2015)

ITU-T World Telecommunication Development Conference WTDC-06 'Mechanisms for enhancing cooperation on cybersecurity, including combatting spam' (Document 116 (Rev.5)-E (12 April 2006) https://ccdcoe.org/sites/default/files/documents/ITU-060315-CoopInCSpam.pdf (date of use: 30 November 2015)

Iweriebor E.E.G 'The colonization of Africa' http://exhibitions.nypl.org/africanaage/essay-colonisation-of-africa.html (date of use: 27 December 2015)

Jackson T 'Can Africa fight cybercrime and preserve human rights' http://www.bbc.com/news/business-32079748 (date of use: 27 December 2015)

Japan African Network 'African countries' independence days' http://www.japanafricanet.com/directory/presidents/africanindependence.html (date of use: 27 December 2015)

Kania D 'The art and science of online profiling' http://www.clickz.com/clickz/column/1702454/the-art-and-science-of-online-profiling (date of use: 10 November 2015)

Kassner M 'The truth behind those Nigerian 419 scammers' http://www.techrepublic.com/blog/it-security/the-truth-behind-those-Nigerian-419-scammers (date of use: 6 November 2015)

Kapersky Lab 'Malware classifications' http://www.kaspersky.co.za/threats/what-is malware (date of use: 10 November 2015)

Kruger H 'The Top 10 Scam types in South Africa' http://www.junkmail.co.za/blog/the-top-10-scam-types-in-south-sfrica/6897 (date of use: 6 November 2015)

Lohman T 'ACMA to force anti-spam on ISPs' http://www.itnews.com.au/News/36262,acma-to-force-anti-spam-on-isps.aspx (date of use: 15 January 2016)

Lynch K 'Timeline of spam related terms and concepts' http://keithlynch.net/spamline.html (date of use: 5 November 2015)

Macharia J 'Africa needs a cybersecurity law but AU's proposal is flawed, advocates say' http://techpresident.com/news/wegov/24712/africa-union-cybersecurity-law-flawed (date of use: 27 December 2015)

Mann J 'Spam is 95% e-mail traffic says Barracuda' http://www.techspot.com/news/28226-spam-is-95-of-e-mail-traffic-says-barracuda.html (date of use: 07 September 2015)

Matthes C 'Unpacking the POPI Act: The ins and outs of protecting personal information'http://www.itweb.co.za/index.php?option=com content&view=article&id=71001 (date of use: 28 January 2016)

Mawson N 'DMASA database 'leaked'' http://www.itweb.co.za/ index.php?option=comcontent&view=article&id=44060 (date of use: 28 January 2016)

Mawson N 'Finally, a national opt-out list' http://www.itweb.co.za/index.php?id=69237 (date of use: 28 January 2016)

Mawson N 'No decision on opt-out registry yet' http://www.itweb.co.za/index.php?option=comcontent&view=article&id=47451 (date of use: 28 January 2016)

Mbuvi D 'African countries propose stringent rules governing ecommerce and data' http://www.cio.co.ke/news/main-stories/african-countries-propose-stringent-rules-governing-ecommerce-and-data (date of use: 27 December 2015)

McNamee T; Mills G; and Pham J.P 'Morocco and the African Union: prospects for re-engagement and progress on the Western Sahara' (Discussion paper 1/2013) 1-27 http://www.thebrenthurstfoundation.org/Files/Brenthurst_Commissioned_ Reports/Brenthurst-paper-201301-Morocco-and-the-AU.pdf (date of use 27 December 2015)

Merriam Webster 'Donation' https://www.merriam-webster.com/disctionary/donation (date of use: 6 March 2017).

Merriam Webster 'Scam' http://www.merriam-webster.com/dictionary/scam (date of use: 6 November 2015)

Michaelsons 'POPI commencement date or POPI effective date' http://www.michaelson.co.za/blog/popi-commencement-date-popi-effective-date/13109 (date of use: 28 January 2016)

Michaelson 'POPI signed by the President' http://www.michaelson.co.za/blog/popi-signed-by-the-president/12625 (date of use: 20 January 2016).

Microsoft 'Fix your hijacked web browser' http://www.microsoft.com/security/pc security/browser-hijacking.aspx (date of use: 10 November 2015)

Mochiko T 'Cybersecurity: oversharers anonymous' http://www.financialmail.co.za/features/2014/11/06/cyber-security-overshares-anonymous (date of use: 20 January 2016)

Molefi N 'Consumers ripped off by spam SMSes' http://www.sabc.co.za/news/a/ce063b8041dfe949a29eaf1c2eddf908/Consumers-ripped-off-by-spam-SMSes-20131811 (date of use: 20 January 2016)

Mybroadband 'SA spammer pays R65 000 to settle case' http://mybroadband.co.za/news/internet/104657-sa-spammer-pays-r65000-to-settlecase-case.html (date of use: 20 January 2016)

Mybroadband 'Spam opt-out lists: TrustFabric versus DMASA' http://mybroadband.co.za/news/general/47560-spam-opt-out-trustfabric-versusdmasa.html (date of use: 20 January 2016)

Mybroadband 'Spam SMS: why South Africans pay to reply 'stop'' https://mybroadband.co.za/news/smartphones/136828-spam-sms-why-south-africans-pay-to-reply-stop.html (date of use: 6 March 2017)

Ndomo A 'Regional Economic Communities in Africa: a progress overview' (May 2009) http://www2.gtz.de/wbf/4tDx9kw63gma/RECS_Final_report.pdf (date of use: 9 December 2015)

Nedbank 'Scams' http://www.nedbank.co.za/web site/content/crimeawareness/scams.asp (date of use: 6 November 2015)

Nigerian scams 'West Africa scam/Nigeria advance fee fraud in Internet web mail frauds and email letter scam' http://www.crimes-of-persuasion.com/Crimes/Business/nigerian.htm (date of use: 6 November 2015)

Nigeria: The 419 Coalition Web site 'the Nigerian scam (419 advance Fee fraud) defined' at http://home.rica.net/alphae/419coal/ (Date of use: 5 November 2015)

OECD 'About the OECD' http://www.oecd.org/about (date of use: 30 November 2015)

OECD 'OECD invites five countries to membership talks, offers enhanced engagement to other big players' http://www.oecd.org/southafrica/southafricaandtheoecd.htm (date of use: 9 December 2015)

OECD 'OECD launches anti-spam toolkit and invites public contributions' http://www.oecd.org/internet/ieconomy/oecdlaunchesanti spamtoolkitandinvitespubliccontributions.htm (date of use: 30 November 2015)

OECD 'Organisation for European Economic Co-operation' http://www.oecd.org/general/organisationforeuropeaneconomicco-operation.htm (date of use: 9 December 2015)

OECD Council at Ministerial Level 'OECD 50th Anniversary Vision Statement' (C/MIN(2011)6) 1-4 http://www.oecd.org/mcm/48064973.pdf (date of use: 9 December 2015)

OnGuardOnilne.gov 'Spam' http://www.onguardonline.gov/spam.html. (date of use: 6 November 2015)

Olshanlaw 'FTC and UK Head sign MOU signaling cross border Privacy enforcement' http://www.olshanlaw.com/blogs-Advertising-Law-blog,FTC-UK-Cross-Border-Privacy (date of use: 30 December 2015)

Patel A 'How spammers get your number' http://www.citypress.co.za/business/how-spammers-get-your-number/ (date of use: 10 November 2015)

Postel J 'On the junk mail problem' Network Working Group (SRI-ARC) Request for Comment 706 (Nov 1975) NIC #33861, http://www.rfc-archive.org/getrfc.php?rfc=706 (date of use: 5 November 2015)

Proome J 'SA e-mail spam percentage revealed' http://mybraodband.co.za/news/security/58901-sa-e-mail-spam-percentage-revealed.html (date of use: 7 September 2015)

Questia 'Four strategic pillars to guide the African Union: Commission's activities 2009-2012' https://www.questia.com/magazine/1G1-203770101/four-strategic-pillars-to-guide-the-african-union (date of use: 9 December 2015)

Quirk 'What is eMarketing and how is it better than traditional marketing?' https://www.quirk.biz/resources/88/What-is-eMarketing-and-how-is-it-better-than-tradional-marketing (date of use: 5 November 2015)

Rahul.net 'Overview of spam from Lipsitz' http://www.rahul.net/falk/Lip (date of use: 10 November 2015)

Rao JM and Reiley D 'The Economics of spam' http://www.davidreiley.com/papers/SpamEconomics.pdf (date of use: 7 September 2015)

Raz U 'How spammers harvest e-mail addresses' http://www.private.org.il/harvest.html (date of use: 10 November 2015)

Reference 'What does the phrase 'surf the Internet' mean' https://www.reference.com/technology/phrase-surf-internet-mean-8bf3144adff725c (date of use: 3 March 2017)

Reese M 'Warning signs of ponzi schemes: part 2' http://www.moneyweb.co.za/archive/part-2-warnings-signs-of-ponzipyramid-schemes (date of use: 6 November 2015)

Right2Know Campaign 'R2K submission on draft cybercrimes and cybersecurity Bill' http://www.r2k.org.za/2015/11/30/cybercrimesbill (date of use: 28 January 2016)

Rimmer SW 'Death of spam: a guide to dealing with unwanted e-mail' http://www.mindworkshop.com/nospam.html (date of use: 6 November 2015)

Roigas H 'Mixed feedback on the African Union Convention on Cyber security and Personal Data Protection' https://ccdcoe.org/mixed-feedback-african-union-convention-cyber-security-and-personal-data-protection.html (date of use: 9 December 2015)

Rutgers 'Chain letters' http://www.cs.rutgers.edu/~watrous/chain-letters.html (date of use: 5 November 2015)

SADC 'Member states' http://www.sadc.int/member-states (date of use: 9 December 2015)

SARS 'Scams and phishing attacks'

http://www.sars.gov.za/TargTaxCrime/Pages/Scams-and-Phishing.aspx?k=SARSScamSource%3Aemail (date of use: 6 November 2015)

Scambusters.org 'Internet scams, identity theft, and urban legends: are you at risk?' http://www.scambusters.org (date of use: 6 November 2015)

Singel R 'April 12, 1994: Immigration lawyers invent commercial spam' https://www.wired.com/2010/04/0412canter-siegel-usenet-spam (date of use: 6 November 2015)

Shcherbakova T; Vergelis M & Demidova N 'Spam and phishing in the first quarter of 2015' https://securelist.com/analysis/quarterly-spam-reports/69932/spam-andphishing-in-the-first-quarter-of-2015 (date of use: 10 November 2015).

Solomon D 'Harvesting e-mail addresses' http://www.businesstoolchest.com/articles/data/20010305130908.shtml (date of use: 10 November 2015)

South African History Online (SAHO) 'The impact of colonialism' http://www.sahistory.org.za/topic/impact-colonialism (date of use: 27 December 2015)

Suchet P 'Real time online profiling' http://www.clickz.com/clickz/column/1718804/real-time-online-profiling (date of use: 10 November 2015)

Sullivan B 'Preventing a brute force or dictionary attack: how to keep the brutes away from your loot' http://www.codeproject.com/Articles/17111/Preventing-a-BruteForce-or-Dictionary-Attack-How (date of use: 10 November 2015)

Surf-in-the-Sprit 'How spammers reap what you sow' http://www.surfinthespirit.com/the-web/harvesting.html (date of use: 10 November2015)

Snopes.com 'Chain Linked' http://www.snopes.com/luck/chain.asp (date of use: 5 November 2015)

Snopes.com 'Lights out' http://www.snopes.com/crimes/gangs/lightsout.asp (date of use: 5 November 2015)

Snopes.com 'Petitions' http://www.snopes.com/inboxer/petition/internet.asp (date of use: 5 November 2015)

Snopes.com 'Thousand dollar bill' http://www.snopes.com/inboxer/nothing/billgate.asp (date of use: 5 November 2015)

South African Government 'Justice publishes draft cybercrime and cybersecurity Bill for public comments' (28 August 2015) http://www.gov.za/speeches/justice-publishes-cybercrimes-and-cybersecurity-bill-public-comments-28-aug-2015-0000 (date of use: 28 January 2016)

SouthAfrica.info 'Ponzi scheme money frozen' http://www.southafrica.info/news/business/690383.htm (date of use: 6 November 2015)

South China Morning Post 'Australian anti-spam law sparks fierce criticism' http://www.scmp.com/article/437282/australian-anti-spam-law-sparks-fierce-criticism (date of use: 15 January 2016)

SPAMFighter 'ACMA Unleashes SpamMATTERS: the new anti-spam button' http:/ New-Anti-Spam-Button.htm (date of use: 20 January 2016).

Spamhaus 'About Spamhaus' https://www.spamhaus/organization (date of use: 30 November 2015)

Spamhaus 'Australian Spam Act nails first spammer' http://www.spamhaus.org/news/article/161/australian-spam-act-nails-first-spammer (date of use: 15 January 2016)

Spamhaus 'Spamware' http://www.spamhaus.org/whitepapers/spamware (date of use: 10 November 2015)

Spamhaus 'The Definition of Spam' http://www.spamhaus.org/consumer/definition (date of use: 30 December 2015)

Spamhaus 'The top 10 worst spam countries' https://www.spamhaus.org/statistics/countries (date of use: 12 March 2017).

Spamhause 'The world's worst spammers' http://www.spamhause.org/statistics/spammers (date of use: 7 September 2015)

Spam Laws 'Spamlaws: how to stop scams and fraud' http://www.spamlaws.com (date of use: 7 September 2015)

Spamlaws 'Spam laws' http://www.spamlaws.com (date of use: 30 December 2015)

Spamlaws.com 'The purpose of chain letter scams' http://www.spamlaws.com/chain-letter-scam-purpose.html (date of use: 5 November 2015)

Systems Publishers 'South African spam summit announced' http://www.bizcommunity.com/Article.aspx?c=16&1=196&ai=2347 (date of use: 7 September 2015)

Talton B 'The challenge of decolonization in Africa' http://exhibitions.nypl.org/africanaage/essay-challenge-of-decolonization-africa.html (date of use: 27 December 2015)

Tamarkin E 'The AU's cybercrime response: a positive start, but substantial challenges ahead' Policy Brief 73 1-8 (January 2015) https://www.issafrica.org/publications/policy-brief/the-aus-cybercrime-response-a-positive-start-but-substantial-challenges-ahead (date of use: 27 December 2015)

Tay L 'ACMA launches spam SMS reporting tool' http://www.itnews.com.au/News/214731,acma-launces-spam-sms-reporting-tool.aspx (date of use: 20 January 2016)

Technopedia 'Interface Message Processor (IMP) https://www.technopedia.com/definition/7692/interface-messag-processor-imp (date of use: 18 March 2017)

TechTarget 'Header' http://whatis.techtarget.com/definition/header (date of use: 4 March 2017)

TechTarget 'Malware (malicious software)' http://searchsecurity.techtarget.com/definition/malware (date of use: 6 November 2015)

Techtarget 'Snoopware' http://www.whatis.techtarget.com/definition/snoopware (date of use: 10 November 2015)

TechTarget 'UBE (unsolicited bulk email) definition' http://searchcio.techtarget.com/definition/UBE (date of use: 30 December 2015)

Techterms 'Freeware' http://www.techterms.com/definition/freeware (date of use: 10 November 2015)

TechTerms 'Smishing' http://www.techterms.com/definition/smishing (date of use: 6 November 2015)

TechTerms 'SMS' https://techterms.com/definitions/sms (date of use: 10 November 2015)

Templeton B 'Origin of the term 'spam' to mean net abuse' http://www.templetons.com/brad/spamterm.html (date of use: 05 November 2015)

Templeton B 'Reaction to the DEC spam of 1978' http://www.templetons.com/brad/spamreact.html (date of use: 5 November 2015)

The Age 'Aust program being tested to identify spammers' http://www.theage.com.au/articles/2004/12/01/1101577531043.html (date of use: 20 January 2016).

The FBI (San Francisco Division) 'Sanford Wallace indicted for spamming Facebook users' 1-2 https://www.fbi.gov/sanfrancisco/press-releases/2011/sanford wallace-indicted-for-spamming-facebook-users (date of use: 10 November 2015)

The Christian Science Monitor 'White South Africans use Facebook in campaign to return to Holland' http://www.csmonitor.com/World/Africa/2010/0517/white-South-Africans-use-Facebook-in-campaign-to-return-to-Holland (date of use: 5 November 2015)

The Guardian 'Racism row over South Africa school's alleged hair policy' https://www.theguardian.com/world/2016/aug/29/south-africa-pretoria-high-school-for-girls-afros (date of use: 1 September 2016).

The Museum of Hoaxes 'Charles Ponzi and the Ponzi scheme' http://hoaxes.org/archive/permalink/charles_ponzi_and_the_ponzi_scheme (date of use: 06 November 2015)

The Register 'Spanking Spam King: Sanford Wallace faces jail for Facebook flood' http://theregister.co.uk/2015/08/25/spammer_wallace_faces_jail_facebook_scam (date of use: 10 November 2015)

The Sydney Morning Herald 'World's biggest spammer' faces Brisbane court' http://www.smh.com.au/technology/security/worlds-biggest-spammer-faces-brisbane-court-20091216-kwe3.html (date of use: 20 January 2016)

This Day Live 'CPC, EFCC, US Agency sign on consumer protection' http://www.thisdaylive.com/articles/cpc-efcc-us-agency-sign-mou-on-consumer-protection/157613 (date of use: 30 December 2015)

Tin Can Communications 'Unsolicited advertising material bothers 74% of South African consumers' http://www.bizcommunity.com/Article.aspx?c=19&=196&ai=1877 (date of use: 7 September 2015)

TouchBasePro 'Impact of the Consumer protection Act on your e-mail marketing' 1-16 http://creativeengineeringstudio.com/wp-content/uploads/2015/06/Impact-of-the-Consumer-Protection-Act-on-your-Email-MarketingTouch_BasePro_May2011.pdf (date of use: 20 January 2016)

TrustFabric 'About Us' https://www.trustfabric.com/about (date of use: 28 January 2016)

Uchenna JO 'Multilateral legal responses to cyber security in Africa: any hope for effective international cooperation?' Paper presented at the 7th International Conference on Cyber Conflict (2015) 105-117 https://ccdcoe.org/cycon/2015/proceedings/08_orji.pdf (date of use: 27 December 2015)

Ugwu P 'Analyst picks holes in proposed AU Cybersecurity Convention' http://www.nigeriacommunicationsweek.com.ng/e-business/analyst-picks-holes-in-proposed-au-cybersecurity-convention (date of use: 27 December 2015)

UNECA 'CEN-SAD Community of Sahel-Saharan states' http://www.uneca.org/oria/pages/cen-sad-community-sahel-saharan-states-0 (date of use: 9 December 2015)

UNECA COMESA Common Market for Eastern and Southern Africa Protocols/ Treaties http://www.uneca.org/oria/pages/uma-arab-maghreb-union-0 (date of use: 9 December 2015)

UNECA 'EAC Eastern African Communities' http://www.uneca.org/oria/pages/eac east-african-community-0 (date of use: 9 December 2015)

UNECA 'ECCAS Economic Community of Central African States' http://www.uneca.org/oria/pages/eccas-economic-community-central-african-states-0 (date of use: 9 December 2015)

UNECA 'History and background of Africa's regional integration efforts' http://www.uneca.org/oria/pages/ecowas-economic-community-west-african-states-0 (date of use: 9 December 2015)

UNECA 'Regional integration tenets and pillars' http://www.uneca.org/oria/pages/regional-integration-tenets-and-pillars (date of use: 9 December 2015)

UNECA 'SADC Southern African Development Community' http://www.uneca.org/oria/pages/sadc-southern-african-development-community-0 (date of use: 9 December 2015)

UNECA 'UMA Arab Maghreb Union: Treaty/Protocols' http://www.uneca.org/oria/pages/uma-arab-maghreb-union-0 (date of use: 9 December 2015)

United Nations Economic Commission for Africa (UNECA) 'History and background of Africa's regional integration efforts' http://www.uneca.org/oria/pages/history-background-africas-regional-integration-efforts (date of use: 9 December 2015)

Urban Dictionary 'Spamvertise' http://www.urbandictionary.com/define.php?term=spamvertise (date of use: 10 November 2015)

Usenet.org 'What is Usenet?' http://www.usenet.org (date of use: 3 March 2016)

US Securities and Exchange Commission 'Ponzi schemes' http://www.sec.gov/answers/ponzi.htm (date of use: 6 November 2015)

US Securities and Exchange Commission 'Pyramid schemes' http://www.sec.gov/answers/pyramid.htm (date of use: 5 November 2015)

Van Zyl G 'Adoption of the 'flawed' AU cybersecurity convention postponed' http://www.itwebafrica.com/ict-and-governance/523-africa/232273-adoption-of-flawed-au-cybersecurity-convention-postponed (date of use: 9 December 2015)

Vere A 'Legal and Regulatory frameworks for the knowledge economy: concept paper' E/ECA/CODIST/1/15 (29 March 2009) http://repository.uneca.org/bitstream/handle/10855/3452/Bib-27924.pdf?sequence=1 (date of use: 9 December 2015)

Vermeulen J 'Killing spam softly: POPI in South Africa' http://www.broadband.co.za/news/telecoms/81759-killing-spam-softly-popi-in-south-africa.html (date of use: 28 January 2016)

Victoria Legal Aid 'Penalty units' http://www.legalaid.vic.gov.au/find-legal-answers/fines-and-infringements/penalty-units (date of use: 15 January 2016)

Walker F 'Even the new anti-spam laws won't stop those pesky emails' http://www.spamstop.com.au/spam-stop-articles/2004/2/7/even-new-antispam-laws-wont-stop-those-pesky-emails (date of use: 15 January 2016)

Wanli MA; Dat T; Dharmendra S; and Sen L 'Hoodwinking spam email filters' (Proceedings of the 2007 WSEAS International Conference on Computer engineering and Applications Australia January 17-19 2007) 533-537 http://www.researchgate.net/profile/Dat_Tran11/publication/255665198.Hoodwinkin_Spam_Email_Filters/links/54087f860cf2c48563bdc37f.pdf (date of use: 26 November 2015)

Washington Times 'Spammers turn to 'dictionary attacks' http://www.washingtontimes.com/business/20040505-092614-5432r.htm (date of use: 10 November 2015)

Webopedia 'Adware' http://www.webopedia.com/TERM/A/adware.html (date of use: 10 November 2015)

Webopedia 'Arpanet' http://webopedia.com/TERM/A/ARPANET.html (date of use: 6 November 2015)

Webopedia 'Big data' http://www.webopedia.com/TERM/B/big_data.html (date of use: 4 March 2017)

Webopedia 'Keylogger' http://www.webopedia.com/TERM/K/keylogger.html (date of use: 10 November 2015)

Webopedia 'Phishing' http://www.webopedia.com/TERM/P/phishing.html (date of use: 6 November 2015)

Webopedia 'Shareware' http://webopedia.com/TERM/shareware.html (date of use: 10 November 2015)

Webopedia 'Spider' http://www.webopedia.com/TERM/S/spider.html (date of use: 10 November 2015)

Webopedia 'Spyware' http://www.webopedia.com/sgsearch/results?cx=partneTEr pub-8768004398756183%3A6766915980&cof=FORID%3A10&ie=UTF 8&q=spyware (date of use: 10 November 2015)

Webopedia 'Spyware' http://www.webopedia.com/TERM/S/spyware.html (date of use: 10 November 2015)

Webopedia 'The difference between a computer virus, worm and Trojan horse' http://www.webopedia.com/DidYouKnow/Internet/2004/virus.asp (date of use: 5 November 2015)

Webopedia 'What is big data?' http://www.webopedia.com/TERM?B/big_data.html (date of use: 7 September 2016)

Webopedia 'Zombie' http://www.webopedia.com/TERM/Z/zombie.html (date of use: 6 November 2015)

Webster M 'Scam' http://www.merriam-webster.com/dictionary/scam (date of use: 6 November 2015)

WhatIs.com 'Memorandum of understanding (MOU or MoU)' http://whatis.techtarget.com/definition/memorandum-of-understanding-MOU-or-MoU (date of use: 5 December 2015)

White House Fact sheet: 'President Bush signs anti-spam law' http://www.whitehouse.gov/news/releases/2003/12/print/20031216-4.html (date of use: 30 December 2015)

WiseGeek 'What is bulk email?' http://www.wisegeek.com/what-is-bulk-email.htm (date of use: 10 November 2015)

Wired 'Spam king' https://archive.wired.com/wired/archive/4.02/spam.king_pr.html. (date of use: 10 November 2015)

WhatIs.com 'Anti-syware software' http://whatis.techtarget.com/definition/anti spyware-software (date of use: 10 November 2015)

WhatIs.com 'Definition header' http://whatis.techtarget.com/def/header (date of use: 30 November 2015)

WSIS Geneva 2003-Tunis 2005 16-18 November 2005 'Tunis Commitment' http://www.itu.int/wsis/docs2/tunis/off/7.html (date of use: 30 November 2015)

ZDNet 'Anti-spam assault spans Asia-Pacific' http://www.zdnet.com/article/anti spam-assualt-spans-asia-pacific (date of use: 15 January 2016)

ZDNet 'Aust spam enforces turn to forensics for 'dobbing' campaign' http://www.zdnet.com/article/aust-spam-enforcers-turn-to-forensics-for-dobbingcampaign/ (date of use: 20 January 2016)

INDEX PAGE

African Union **108-109; 114-124**
AU Convention on Cyber security and Personal 116-117
Regional Integration 109-113
Penalties 122-123

ATU 112-113
Cooperation 135-137

Australia 196-216
Anti-spam provisions 196-217
Benefits 217-218
Cases 203-206; 216-218
Civil penalties 206-208
Criticisms 218-220
E-marketing code 225-228
Enforcement 210-217
Industry measures 224-225
International cooperation 229-235
Korea 230
New Zealand 235
Seoul and Melbourne 231-232
Taipei 233-235
Thailand 232
UK and USA 232-233

COMESA **111**
Model Law and Guide 125-129

Consumer protection
COMESA 125
ECT Act 239-240
SADC 131

Consumer education and awareness
ITU 85-86
OECD 97-100
Australia 221-224

Contextualisation and commentary
African region 137-139
African Union 117-124
Australia 217-220
COMESA 126-127
ITU and OECD 104-106
SADC 132-134
South Africa 296-301
USA 179-188

State level 158-159

Direct marketing **13-17**
Definitions 13-14; 119; 256; 270
Traditional marketing versus electronic marketing 15-17

Harmonization
ICT Policies in Sub-Saharan Africa 129-130
ITU 80-81
South African 297-301

ITU **57-88**
Enforcement 77-80
ITU-T 59
Multi-pronged approach 64-87
Industry partnership 84
International cooperation 86-87
Penalties 76-77
Strong legislation 64-81
Technical tools 81-84
Study group 17 60

OECD **89-104**
Anti-spam technologies 97
Anti-spam Toolkit 90-91
Cooperative partnerships 100-102
Elements 91-103
Global cooperation 102-103
Industry driven initiatives 96-97
Task force 89-90

Opt-in 116-117
AU 120-121
Australia 198-200
ECT Amendment Bill 283-285
ITU 68-69
POPI Act 271-273
SADC 133-134
USA state level 148-150

Opt-out
Australia 200-201
COMESA 126; 128-129
CPA 258-260
ECT Act 241-242
ITU 69-70; 75-76
SADC 133-134
USA 162-164
State level 150-151

SADC **112; 129-135**
- Model Law on Electronic Transactions 131-134
- Model Law on Computer crimes and Cyber-crimes 134-135

Spam
- ARPAnet 18-20
- Definitions
  - Commercial electronic messages (CEM) 197
  - Commercial communications 282-283
  - Commercial electronic transactions 283
  - Electronic communications 128; 133; 271
  - UBE or UBEM 144-145
  - UBCE 143
  - Unsolicited communications 282
  - UCE or UCEM 143-144
  - UCEA 142
- Dictionary attacks 43-44; 73-74; 157; 171; 204-205; 291-294
- Harvesting 41-42; 73-75; 156-157; 170-171; 201-203; 243-244; 274-277
- Labelling of e-mails 71-73; 151-152; 171-173;
- Lucrative business 33-35
- Malware 292-293
- Methods 37-46
- Nature 145-148
- Online profiling 38-39
  - Use of cookies 40-41
- Problems 46-50
- Spyware 44-45
- Spam fighters 54-55
- Spoofing (fraudulent headers) 46; 70-73; 152-156; 165-170; 200; 244; 273-274; 306-307
- Technical measures 50-54; 228-229
- Types 20-33

UNITED STATES

CAN-SPAM Act 160-194
- Anti-spam provisions 161-179
- Benefits 179-180
- Cases 166-170; 181-184; 186-187
- Criticisms 180-188
- Do-not-email registry 176-177
- Enforcement 173-176
- International cooperation 190-194

Mexico 191
Nigeria 192-193
Spain 191-192
UK 193-194
UK and Australia 190-191
Solutions 188-194
Pre-emption 180-185
State laws 141-159
Anti-spam features 142-159
Cases 153-156
Enforcement and penalties 157-158

SOUTH AFRICA

CPA 253-266
Consumer’s right to privacy 254-255
Direct marketing and the right to privacy 256-258
Do-not-call registry 260-264
Enforcement 265
Penalties 266

Cybercrimes Bills 285-295
Anti-spam provisions 288-294
Enforcement 294

ECT Act 238-253
Anti-spam provisions 241
Amendment Bill 283-285
Benefits 241-242
Case(s) 248-250
Criticisms 242-245
Data protection 240-241
Enforcement 244-245
Penalties 245
Solutions 245-247

POPI Act 266-281
Direct marketing and unsolicited communications 269-280
Directories 277-278
Enforcement 278-280
Penalties 280

Self-regulation
DMASA 262-264
ISPA 250-252