Strengthening e-crime legislation in the UAE:

Learning lessons from the UK and the EU

Waleid Al Antali

M00474208

Submitted in partial fulfilment of the requirements for the degree of Doctor of Philosophy

Middlesex University

School of Law

January 2018

Dedication

My family are the most important persons to me and I dedicate this research to them.

Acknowledgements

First and foremost, I would like to express my sincere gratitude to my supervisors: Professor Julia Davidson, Dr Elena Martellozzo and Renu Barton-Hanson, Associate Professor of Law. I feel honoured to have been their PhD student. I appreciate all the time, helpful suggestions and ideas which have made my studies extremely stimulating. The continuous support, motivation and immense knowledge of my supervisors and dedication to their role was unparalleled. Much gratitude for the most helpful discussions. The guidance and mentoring I received from my supervisors was truly outstanding.

Thank you to Middlesex University London which provided me with a fantastic academic environment for my research. I have the fondest memories of my research time. My time at Middlesex University also allowed me to make wonderful new friends.

Additionally, I am immensely appreciative to my expert research interviewees, who have shared their knowledge and expertise with me. Thank you for agreeing to participate in my research. Your contributions were invaluable and formed the foundation of my research.

I am indebted to His Highness Sheikh Khalifa bin Zayed Al Nahyan. Completion of this PhD would not have been possible without the excellent education I received, as well as the support which furthered my academic pursuits. I would also like to take the

opportunity to acknowledge that I was very privileged to be taught by many excellent teachers.

I am deeply grateful to my family and friends for surrounding me with the love and encouragement I needed during this challenging period of my life. I would especially like to thank my dear sister Ibtissam and my loyal friend Mohamed for their unwavering support in helping me to meet this goal.

Abstract

The electronic revolution brought with it technological innovations that are now integral to communication, business, commerce and the workings of governments all over the world. It also significantly changed the criminal landscape. Globally it has been estimated that crime conducted via the internet (e-crime) costs more than €290 billion annually. Formulating a robust response to cybercrime in law is a top priority for many countries that presents ongoing challenges. New cybercrime trends and behaviours are constantly emerging, and debates surrounding legal provisions to deal with them by increasing online tracking and surveillance are frequently accompanied by concerns of the rights of citizens to freedom, privacy and confidentiality. This research compares the ways that three different legislative frameworks have been navigating these challenges. Specifically, it examines the legal strategies of the United Arab Emirates (UAE), the United Kingdom (UK) and the European Union (EU). The UAE is comparatively inexperienced in this area, its first law to address e-crime was adopted in 2006, sixteen years after the UK, and so the express purpose of this study is to investigate how e-crime legislation in the UAE can be strengthened. Drawing on a range of theoretical resources supplemented with empirical data, this research seeks to provide a comprehensive account of how key e-crime legislation has evolved in the UAE, the UK and the EU, and to evaluate how effective it has been in tackling cybercrime. Integral to this project is an analysis of some of the past and present controversies related to surveillance, data retention, data protection, privacy, non-disclosure and the public interest. An important corollary of this research is how e-

crime legislation is not only aligned with political and economic aims, but when looking at the UAE, the discrete ways that legislation can be circumscribed by cultural, social and religious norms comes into focus.

Abbreviations

ACPO	Association of Chief Police Officers
CFR	Charter of Fundamental Rights
CJEU	Court of Justice of the European Union
CPS	Crown Prosecution Service
DDoS	Distributed Denial of Service
DIFC	Dubai International Financial Centre
DPP	Director of Public Prosecution
DRIPA	2014 Data Retention and Investigatory Powers Act 2014
Du	Emirates Integrated Telecommunications Company
EC3	European Cybercrime Centre
ECHR	European Convention on Human Rights
EEA	European Economic Area
ENISA	European Network and Information Security Agency
Etisalat	Emirates Telecommunications Corporation
FATF	Financial Action Task Force
FSC	Federal Supreme Court
GCC	Gulf Cooperation Council
GCHQ	Government Communications Headquarters
GDPR	General Data Protection Regulation
IP	Intellectual Property

IPS	Internet service providers
IPT	Investigatory Powers Tribunal
IT	Information technology
ITCs	Information Communication Technologies
NPCC	National Police Chiefs Council
NSA	National Security Agency
NESA	National Electronic Security Authority
PACE	Police and Criminal Evidence Act 1984
RIPA	Regulation of Investigatory Powers Act 2000
SIAs	Security and Intelligence Agencies
SOCA	Serious Organised Crime Agency
SCEDEA	Scottish Crime and Drug Enforcement Agency
UK	United Kingdom
UAE	United Arab Emirates
VoIP	Voice Over Internet Protocol
VPN	Virtual Private Network

Table of Contents

Dedication **2**

Acknowledgements **3**

Abstract **5**

Abbreviations **7**

Table of Contents **9**

Chapter One: Introduction and Literature Review **13**

1. Introduction 13

1.1 The Significance and Importance of the Research Topic 15

1.2 The Scope of the Research 21

1.3 Research Aim and Objectives 25

1.4 Structure of the Thesis 26

1.5 Defining Cybercrime 29

1.6 The Theoretical Context of and Applicable Social Science Literature on Cybercrime 37

1.7 Cybercrime Laws in the UK 49

1.8 The European Approach Towards Cybercrime 56

1.9 Cybercrime Laws in the UAE 63

1.10 The UK Approach Towards Data Protection 71

1.10.1 The Right to Privacy 71

1.10.2 The UK Data Protection Act 1998 and the European Approach Towards Maintaining Privacy 79

1.10.3 The 2012 European Reform Proposals 84

1.11 Surveillance Laws in the UK 88

1.12 Surveillance Laws in the UAE 98

1.13 The UK and European Approach Towards Data Retention 100

1.14 The UK Evidence Rules on Admissibility for Criminal Proceedings 111

1.14.1 The UK Evidence Rules Governing Circumstances of Public Policy Non-Disclosure 118

1.15 Summary 123

Chapter Two: Methodology 127

2. Introduction 127

2.1 Ontology 129

2.2 Epistemology 139

2.3 Research Philosophy 141

2.4 Research Choices 142

2.5 Research Design, Approach and Strategy 143

2.6 Doctrinal Legal Analysis 145

2.7 Comparative Legal Research 147

2.8 Empirical Legal Research 148

2.9 Researching Sensitive Issues and Ethics 149

2.10 Qualitative Interviewing 156

2.11 Sampling 158

2.12 Conducting the Interviews and Recording the Data 163

2.13 Data Quality 164

2.14 Data Analysis 170

2.15 Publishing Qualitative Research 173

2.16 Summary 173

Chapter Three: The UK's Main Computer Misuse Offences, RIPA Policing Powers, Data Retention and Public Interest Immunity 178

3. Introduction 178

3.1 The Computer Misuse Act 1990 179

3.2 Interception, Surveillance, Communications Data Acquisition and Decryption and the UK Regulation of Investigatory Powers Act 2000 (RIPA) 195

3.2.1 RIPA and Interception 202

3.2.2 RIPA and Surveillance 207

3.2.3 RIPA and Decryption 212

3.4 Data Retention: The EU Data Retention Directive, the UK Data Retention and Investigatory Powers Act 2014 and the Investigatory Powers Act 2016 214

3.5 Admissibility of Intercepted Communication in Court Proceedings 226

3.6 Summary 230

Chapter Four: The UAE's Legislative Framework to Combat E-Crime 233

4. Introduction 233

4.1 The UAE's Legislative E-Crime Framework 240

4.2 The Criminal Procedure Law and Procedural Rules Governing Electronic Evidence 259

4.3 Summary 274

Chapter Five: Understanding How to Strengthen E-Crime Legislation in the UAE Through Interviews with Senior E-Crime Experts 278

5. Introduction 278

5.1 Discussion and Analysis of The Qualitative Interviews 280

5.1.1 Key Findings and the Relevant Literature 280

5.1.2 Legislation for Cybercrime Offences 285

5.1.3 Surveillance and Data Retention Laws 303

5.1.4 Privacy and Data Protection 318

5.1.5 Evidence Rules on the Admissibility of Digital Evidence and Intercept Material in Criminal Proceedings 322

5.2 Summary 324

Chapter Six: Developing a Legal Framework to Combat E-Crime in the UAE 325

6. Introduction 325

6.1 Surveillance: Towards a More Preventative and Intelligence-Led Policing Model 327

6.2 Privacy, Data Protection and Security 346

6.3 Federal Law No. 5 of 2012 Concerning Combating Information Technology Crimes 354

6.4 The Criminal Procedure Law and Procedural Rules Governing Electronic Evidence 358

6.5 Cooperation 364

7. Conclusion 370

8. Recommendations 381

9. Bibliography 387

10. Appendices 488

10.1.1 Interview Schedules 489

10.1.2 Interview Information Sheet and Consent Form 504

10.1.3 Example of an Interview Request to a UK Expert 506

10.1.4 Response Received from a UK Expert to an Interview Request 507

Chapter One: Introduction and Literature Review

1. Introduction

This Chapter explains the importance of the research. It addresses the topics covered by the research, i.e. its scope. Next, the research objectives are presented, followed by an overview of the theoretical context and the literature. The purpose of the literature review is to identify the core issues from the existing literature with respect to the research topic. To this end, a systematic review was conducted and the most recent books and papers were consulted in order to identify key legislation, to highlight any controversies and the latest developments, including reform proposals in the research area. The literature review draws together a variety of different components - cybercrime offences surveillance, data acquisition and retention, data protection, network and information security and evidence laws – that are crucial to the formulation of a comprehensive legislative framework to combat cybercrime. Specifically, the researcher made extensive use of WestLaw, LexisNexis and HeinOnline, and searched various journals, such as, the Police Journal, the Computer and Telecommunications Law Review, the Archbold Review, Communications Law, the European Human Rights Law Review, the Ethics and Information Technology, the Criminal Law Review, the European Law Review, Privacy & Data Protection and EU Focus.

In terms of the structure, recourse is made to previous research about cybercrime laws, surveillance and data retention and protection laws in the UAE, UK and EU, as well as UK evidence law rules dealing with admissibility of electronic evidence and intercepted communications in criminal court proceedings to prosecute cyber criminals. The reason for this is that whilst cybercrime laws proscribe distinct offences, they do not constitute the entire legal arsenal necessary to combat cybercrime effectively and to successfully prosecute cyber criminals. Grady et al (2007) opine that *"policymakers recognise that criminalising specific activities is not a complete or sufficient response to the threat of hackers, virus writers and cyber-terrorists"* and *"policymakers have recognised the need to facilitate cybersecurity through a variety of mechanisms, including the imposition of legal obligations*.[1] They explain that, for instance, data protection plays an essential role since data controllers are obligated to adopt security measures, or are required to report security breaches.

Firstly, the literature review defines cybercrime, it examines the theoretical criminological context and reviews the existing social science literature in this area. Secondly, UK cybercrime laws,, the European approach towards cybercrime, as well as cybercrime laws in the UAE are explored. Thirdly, surveillance laws are investigated and the approach taken by both the UK and the UAE on this matter is thoroughly considered. Fourthly, how the UK and the European Union has dealt with the issue of data retention is discussed. Then, the UK approach towards data protection, the right to privacy and the UK Data Protection Act 1998 is examined and followed up with the

[1] M. Grady, F. Parisi, I. Walden, The Law and Economics of Cybersecurity, Publication Review, 13(2) *Computer and Telecommunications Law Review* 2007, 78-79, 78

European stance on maintaining privacy and the 2012 European reform proposals. Finally, UK evidence rules on admissibility for criminal proceedings, as well asthe circumstances in which public policy permits non-disclosure are analysed.

1.1 The Significance and Importance of the Research Topic

The advent of the internet and the widespread use of mobile phones, tablets and computers has not only brought with it many benefits and opportunities, but it has also placed governments, businesses and citizens at risk of criminal activity conducted via the internet (e-crime). Various terminologies can be used to describe e-crime, such as, computer crime, technology crime, online crime, electronic crime, cybercrime, computer related crime, high-tech crime and computer misuse.[2] For the purposes of this thesis the meaning of the terms 'cybercrime' and 'e-crime' is identical, The UK Association of Chief Police Officers (ACPO), now the National Chief Police Council, defines e-crime as *"The use of networked computers or internet technology to commit or facilitate the commission of crime."*[3] It has been estimated that globally e-crime costs €290 billion annually which exceeds the entire illegal sale of heroin, cocaine and marijuana.[4] Research about the development of a comprehensive national legislative framework to combat e-crime is critical, since it can assist governments around the world to formulate

[2] I. Baggili, *Digital Forensics and Cybercrime: Second International ICST Conference, ICDF2C 2010, Abu Dhabi, United Arab Emirates, October 2010, Revised Selected Papers* (London, Springer 2011) 2
[3] House of Commons: Home Affairs Committee, Great Britain Parliament, *House of Commons - Home Affairs Committee: E-Crime - HC 70: Fifth Report of Session 2013-14* (London, TSO Shop 2013) 99
[4] Europol, Cybercrime: A Growing Global Problem, 2014 <https://www.europol.europa.eu/ec/cybercrime-growing> accessed 15 May 2014

an effective response to this newly emerging, and rapidly changing, field by allocating *"certain burdens and benefits among the citizenry."*[5]

Cybercrime research is vital for digital economies around the world. It is an inherently global phenomenon which makes it much more difficult to combat than other traditional forms of crime. Identification of cyber-criminals through digital footprints raises a number of technical problems and prosecution can be very complicated due to jurisdictional issues, such as when certain countries may not yet have drawn up any specific cybercrime offences.[6] Specialised policing and a sophisticated understanding of technological issues needs to be developed to secure the ever expanding and borderless digital world.[7] [8]

Another continuing concern is that no international cybercrime agreement exists apart from the Convention on Cybercrime adopted by the Council of Europe in 2001.[9] There is no comprehensive and up-to-date international guidance available for the development of a strong legislative framework to fight e-crime.[10] With the exception of Interpol[11] and the Virtual Global taskforce (the latter set up to deal with child abuse),[12] there is no other *"global cybercrime law enforcement agency"*. Rather, it is the

[5] W. A. Edmundson, *The Duty to Obey the Law: Selected Philosophical Readings* (Oxford, Rowman & Littlefield Publishers Inc, 1999) 37
[6] R. Miller, F. Cross, *The Legal Environment Today: Business In Its Ethical, Regulatory, E-Commerce, and Global Setting* (7th edn, Mason, South-Western Cengage Learning 2013) 177
[7] C. Hess Orthmann, K. Hess, *Criminal Investigation* (10th edn, Clifton Parl, Delmar Cengage Learning 2013) 522
[8] C. Easttom, *Computer Crime, Investigation, and the Law* (Boston, Cengage Learning 2011) 234
[9] Council of Europe, Convention on Cybercrime 2001 <http://conventions.coe.int/Treaty/en/Treaties/html/185.htm> accessed 7th November 2014
[10] J. Westby, *International Guide to Combating Cybercrime* (Chicago, ABA Publishing 2003) 61
[11] Interpol, Cybercrime, 2014 <http://www.interpol.int/Crime-areas/Cybercrime/Cybercrime> accessed 7th November 2014
[12] Virtual Global Taskforce, 2014 <http://www.virtualglobaltaskforce.com/> accessed 7th November 2014

responsibility of each country to adopt its own cybercrime legislation and to cooperate with each other to prosecute cyber-criminals. Noting that with respect to the EU, the EU Cybercrime Centre has been created.[13]

To create a safe digital space the necessary legal rights, duties and powers have to be clearly demarcated. A comprehensive legislative framework to combat cybercrime does not solely consist of outlawing certain acts as this is insufficient to combat the already mentioned multi-jurisdictional issues that it raises. Data has to be protected and the digital realm has to be surveilled, data also has to be retained and in certain circumstances it has to be admissible in court proceedings, whereas in others, enforcement agencies have to be able to rely on public policy to prevent disclosure. Businesses benefit from the adoption of robust data protection safeguards, as otherwise the commercial exchange of data, which has become very important in the information age, may be hampered.[14] Data protection safeguards make it more difficult for cyber-criminals to commit security breaches, steal sensitive data and helps preventing data loss. These are just some of the complex, diverse and coordinated measures involved in securing cyber-space and the development of a legislative framework to analyse and implement them requires legal scholarship. This is also critical against the backdrop of the recent revelations by Edward Snowden (2014), which highlight that governments

[13] S. W. Brenner, *Cybercrime: Criminal Threats from Cyberspace* (Santa Barbara, Greenwood Publishing Group 2010) 174; Europol, A Collective EU Response to Cybercrime, 2015 <https://www.europol.europa.eu/ec3> accessed 20 February 2015

[14] Also see Pinsent Masons, US to strengthen Safe Harbour framework for personal data transfers from EU by summer, Out-Law.com, 2014 < http://www.out-law.com/en/articles/2014/march/us-to-strengthen-safe-harbour-framework-for-personal-data-transfers-gfrom-eu-by-summer/> accessed 15 June 2014

extensively gather information about their citizens.[15] Edward Snowden acted as a whistle-blower and informed the public of the far-reaching and global secret surveillance activities conducted by the United States National Security Agency (NSA) and other intelligence agencies, and this subsequently sparked a much debate about the legality and constitutionality of digital security and surveillance and their impact on the right to privacy, civil liberties and human rights.

The UAE is no stranger to cybercrime. Many people in the UAE have suffered financial losses from cyber attacks and it has been predicted that these will become more sophisticated.[16] It is therefore crucial that the UAE adopts an equally sophisticated legislative framework to combat e-crime. In 2006, the UAE government adopted the Federal Law No.2 of 2006 on Combating Cybercrime.[17] In 2012, the UAE then passed Law No. 3 of 2012 on Establishing the National Electronic Security Authority and Law No. 5 of 2012 Concerning Combating Information Technology Crimes in order to further improve the legislative landscape.[18] Nevertheless, promotion of a digital economy requires a proactive stance towards combating e-crime, and this in turn means continuously updating and improving legislation. It is for this reason that the research will give critical attention to whether the existing cybercrime laws in the UAE are effective. To assist with this aim the research will foreground the approach adopted by

[15] E. Snowden, What Europe Should Know about US Mass Surveillance, Whistleblower delivers written testimony to European Parliament (*Original.antiwar.com,* 2014) <http://original.antiwar.com/edward-snowden/2014/03/07/what-europe-should-know-about-us-mass-surveillance/> 30 April 2014
[16] EPOC Messe Frankfurt GmbH, UAE to face advanced cybercrime in 2013 <http://www.messefrankfurtme.com/frankfurt/1263/for-journalist/technology-production/intersec-middle-east/industry-news/for-journalists.aspx> accessed 15 May 2014
[17] Gulfnews, Full text of UAE decree on combating cybercrimes, 2012 <http://gulfnews.com/news/gulf/uae/government/full-text-of-uae-decree-on-combating-cyber-crimes-1.1104040> accessed 16 June 2014
[18] Ibid

the UK, as the UK government has been very proactive in its attempts to protect its citizens from cybercrime, as can be seen in the following ways: it follows a national Cyber Security Strategy, [19] it has created a government agency to monitor implementation of the data protection legislation, [20] it has established a National Cybercrime Unit,[21] it carries out data retention[22] and has equipped enforcement agencies with wide powers to utilise the UK's state unlimited surveillance capabilities, and[23] the budget for M15 to conduct research and development in the fields of protective security and surveillance technology has significantly increased. [24] Taking into account that several of these measures taken by the UK government were driven by and/or in response to data retention and protection initiatives taken at the European level, the research will make recourse to the relevant EU directives.

The research will also examine the issue of when digital information can/cannot be used in criminal proceedings to enforce cybercrime laws. The Scientific Working Group of Digital Evidence defines digital evidence as *"information of probative value that is stored or transmitted in binary form*," it includes evidence on any digital device and is

[19] UK Cyber Security Strategy, Protecting and promoting the UK in a digital world, November 2011, 1-43 <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf> accessed 3rd December 2014
[20] Information Commissioner's Office, Data Protection, 2014 <https://ico.org.uk/for_organisations/data_protection> accessed 3rd December 2014
[21] National Crime Agency, National Cybercrime Unit, 2014 <http://www.nationalcrimeagency.gov.uk/about-us/what-we-do/national-cyber-crime-unit> accessed 3rd December 2014
[22] For instance, see the Data Retention and Investigatory Powers Act 2014
[23] C. Cadwalladr, Edward Snowden: state surveillance in Britain has no limits, Guardian, 12 October 2014 <http://www.theguardian.com/world/2014/oct/12/snowden-state-surveillance-britain-no-limits> accessed 1st December 2014
[24] P. Wilkinson, *Homeland Security in the UK: Future Preparedness for Terrorist Attack Since 9/11* (Abingdon, Routledge 2007) 190

not limited to cybercrimes, but extends to traditional crimes.[25] Indeed, the unique nature of digital information raises a number of thorny legal issues, as the search and seizure of electronic data requires adherence to protocols and rules to ensure that the authenticity of the evidence does not become undermined and to regulate the extent to which searches are deemed lawful.[26]

Clearly, not all information, which is being gathered and retained, should be used as electronic evidence in criminal court proceedings. It is imperative that digital information which has been collected at a crime scene is distinguished from covertly collected information used for policing purposes.[27] In certain situations the public interest could be compromised through a disclosure of such information.[28] The adoption of such evidence rules is therefore an important building block to create a framework which reinforces *"impartiality, transparency, effectiveness, and fairness"* in order to promote the rule of law.[29] It also facilitates co-operation between enforcement agencies, including international cooperation, which is crucial to combat cybercrime effectively.[30] Ultimately, the research seeks to contribute to the ongoing, hotly contested and pressing legal debates of how best to secure the digital space. In sum, it is an issue concerning *"update[ing] legislation and regulation in a timely manner [to avoid]...catastrophic*

[25] S. K. Prasad, S. Routray, R. Khurana, *Information Systems, Technology and Management* (Berlin, Springer-Verlag 2009) 179
[26] D. Littlejohn Shinder, M. Cross, *Scene of the Cybercrime* (Burlington, Syngress Publishing Inc 2008) 642-643
[27] J. Sammens, J. Rajewski, *The Basics of Digital Forensics: The Primer For Getting in Digital Forensics* (Elsevier Inc 2012) 46
[28] A. Keane, P. McKeown, *The Modern Law of Evidence* (9th edn, Oxford University Press 2012) 560
[29] J. E. J. Prins, P. M. A. Ribbers, *Trust in Electronic Commerce: The Role of Trust from a Legal, an Organizational and a Technical Point of View* (Kluwer Law International 2002) 277
[30] Council of Europe, Action against economic crime, Resources: International cooperation against cybercrime, 2014 <http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Internationalcooperation/default_en.asp> accessed 3 May 2014

consequences because technology advances occur frequently and subsequent advances in cyber-warfare and cyber-crime keep pace."[31]

1.2 The Scope of the Research

The research aim is to compare the legislative frameworks of the UAE, the UK and the EU, and to consider the most appropriate e-crime framework for the UAE. Integral to this aim is the issue of rendering the digital environment in the UAE safer through improved cybercrime laws. Consequently, the thesis explores and evaluates what appears to be working effectively in the UK and the EU, what are the elements of best practice and how relevant these are for the UAE context. Five senior experts in the field of cybercrime from the UAE are interviewed, namely from the judiciary, the police, Interpol, the office of prosecution and the Telecommunications Regulatory Authority in order to ascertain how effective the existing legislative regime is and how it might be improved. Whilst the UAE has a different culture than the UK and the EU, the thesis does not draw examples from other Middle Eastern countries, such as Bahrain and Qatar, as the fight against cybercrime is global and technical in nature, and thus transcends local traditions and culture.

Cybercrime laws, surveillance, data retention and data protection laws in the UAE, UK and EU, as well as UK evidence law rules dealing with admissibility of electronic evidence and intercept material in criminal court proceedings in order to prosecute cyber-criminals are investigated. Hence, the cybercrime offences, which the UK and

[31] M. Gregory, D. Glance, *Security and the Networked Society* (London, Springer 2013) 1-2

UAE have adopted, as well as the European approach in respect of cybercrime, are critically analysed. UK surveillance laws are discussed in order to identify the powers, which enforcement agencies can utilise to investigate cybercrime. Additionally, UK and European data retention laws are reviewed, as they form an integral part in the fight against cybercrime.[32] The UK legal framework to secure privacy and data protection, [33] and the European approach towards maintaining privacy are investigated, including the 2012 reform proposals to adequately safeguard personal data and those regarding network and information security. [34] The UK evidence rules on admissibility of electronic evidence are discussed for criminal proceedings, including in relation to covertly collected information. Recourse is made to public policy, which permits non-disclosure in certain circumstances.[35] Hence, the research does not only discuss the cybercrime offences, but also scrutinises the treatment of electronic information and evidence from the perspective of effectively combating cybercrime.

Essentially, the scope of the research is limited to discussing the following: firstly UK and UAE laws which set out e-crime offences and the European approach; secondly the UK laws which permit enforcement agencies to carry out surveillance and other proactive methods to combat cybercrime; thirdly, UK, European and UAE laws which deal with data retention, data protection and network and information security; and fourthly, UK and UAE evidence rules which govern the admissibility of digital evidence

[32] For instance, UK legislation, such as the Regulation of Investigatory Powers Act 2000, which permits companies and enforcement agencies to collect electronic data, will be scrutinised.

[33] R. Subramanian, *Computer Security, Privacy, and Politics: Current Issues, Challenge, and Solutions* (IRM Press 2008) 61

[34] European Commission, Commission proposes a comprehensive reform of the data protection rules, 2012 <http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm> accessed 1st May 2014

[35] A. Keane, P. McKeown, *The Modern Law of Evidence* (9th edn, Oxford University Press 2012) especially Chapter 9

and intercept material in criminal court proceedings. The Sharia Law will not be explored in depth and will not be in the scope of this research. It is noted that the focus will not only be on the traditional form of cybercrime, but also on the more general use of technology and the internet in commiting crimes in the real world. In this sense, as it is discussed in the body of this thesis, and more specifically in the part defining cybercrimes, the term 'cybercrime' for the purposes of this thesis encompasses the use of the internet in facilitating traditional crimes, and for this reason parts of the discussion focus on the use of measures to prevent the facilitation of such 'real world' crimes with the assistance of technology and the internet. It is highlighted that the aim of the thesis is not to cover the full spectrum of cybercrimes, even though reference may be made to different forms of cybercrime, the focus is on network assisted crimes.

As already indicated, the research focuses on the UK, the European Union and the UAE, excluding any other jurisdictions. The UK's key Act is the Computer Misuse Act 1990, as amended by the Police and Justice Act 2006, though various other Acts can be also utilised to bring cyber criminals to justice.[36] The Computer Misuse Act was adopted in 1990, i.e. *"before the cyberspatial explosion that was delivered by the internet"*[37] and a study, which would be limited to this Act, would be too narrow. Instead, the digital realm is rendered more secure in Europe since additional steps have been taken to safeguard the digital space, including through surveillance and data retention.[38] Yet this

[36] J. X. Kelly, Computer Misuse Overview, JISC Legal Information, 2007 <http://www.jisclegal.ac.uk/LegalAreas/ComputerMisuse/ComputerMisuseOverview.aspx> accessed 17 June 2014

[37] N. MacEwan, The Computer Misuse Act 1990: lessons from its past and predictions for its future, 12 *Criminal Law Review* 2008, 955-967, 966

[38] I. M. Portela, M. Manuela Cruz-Cunha, *Information Communication Technology Law, Protection, and Access Rights Global Approaches and Issues* (Hershey PA, IGI Global 2010) 368; A. V. M. Leong, *The*

is not to say that the researcher does not acknowledge the tension that exists between safeguarding fundamental human rights, particularly the right to privacy, on the one hand, and the work by enforcement agencies who conduct surveillance on the other. This is a highly conflictual topic that raises pertinent questions about what data is required by these enforcement agencies and what should be considered permissible in an increasingly technologically-driven world, and as shall be shown in this thesis the answers to these questions are dependent upon cultural and social norms, and political and economic considerations.[39]

The research makes recourse to case law, as well as government strategies, policies, protocols and procedures. A comprehensive legislative framework to combat e-crime has to be complemented by an appropriate government strategy and policies, and it requires enforcement agencies to adopt technical and investigative standards, protocols and procedures.[40] For instance, it is pivotal that particular procedures are followed to ensure that electronic evidence is authentic and in the UK, the ACPO, now the National Police Chiefs Council (NPCC) has published the Good Practice Guide for Digital Evidence 2011, the Good Practice Guide for Computer-Based Electronic Evidence and the Good Practice Guide for Managers of e-Crime investigation.[41] Best practice

---

Disruption of International Organised Crime: An Analysis of Legal and Non-Legal Strategies (Aldershot, Ashgate Publishing Ltd 2007) 171

[39] R. A. Cropf, T. C. Bagwell, *Ethical Issues and Citizen Rights in the Era of Digital Government Surveillance* (Hershey, Information Science Reference 2016) 95

[40] E. U. Savona, Crime and Technology: New Frontiers for Regulation, Law Enforcement and Research (Dordrecht, Springer 2004) 51

[41] The Association of Chief Police Officers Good Practice Guide for Digital Evidence 2012, <http://www.acpo.police.uk/documents/crime/2011/201110-cba-digital-evidence-v5.pdf> accessed 2 May 2014; the Association of Chief Police Officers Good Practice Guide for Computer-Based Electronic Evidence, <http://www.7safe.com/electronic_evidence/ACPO_guidelines_computer_evidence.pdf> 2 May 2014; the Association of Chief Police Officers Good Practice Guide for Managers of e-Crime

guidance has also been adopted for forensics,[42] and whilst the thesis refers to best practice guidance, the technical procedures are not discussed, as this would exceed the scope of this research. The research emphasis is firmly placed on law, as opposed to technology and forensics. Given that the focus is case law, the research does not investigate the way in which cyber-criminals operate or how technology can be employed to capture cyber criminals or to gather digital information; it is not concerned with Information Technology and Information Communications Technology, neither is it concerned with the behaviour of offenders in this context.

1.3 Research Aim and Objectives

The research aim is to comprehensively analyse and to critically compare the legislative frameworks which the UK, the EU and the UAE have adopted to combat e-crime. To meet this research aim an exploration and evaluation of the following topics will be required:

1. UK cybercrime offences legislation.
2. UK surveillance and UK and EU data retention laws.
3. UK and EU privacy, data protection, and network and information security laws.

Investigation, <http://www.acpo.police.uk/documents/crime/2011/201103CRIECI14.pdf> accessed 2 May 2014

[42] For example, see the Codes of Practice and Conduct for forensic science providers and practitioners in the Criminal Justice System, Version 1.0, 2011 <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/118949/codes-practice-conduct.pdf> accessed 2 May 2014; ENFSI Working Group Forensic IT, Guidelines for Best Practice in the Forensic Examination of Digital Technology 2009, <http://www.enfsi.eu/sites/default/files/documents/forensic_it_best_practice_guide_v6_0.pdf> accessed 2 May 2014

4. UK evidence rules on the admissibility of digital evidence and intercept material in criminal proceedings.
5. The effectiveness of UAE's legislative framework to combat e-crime.

It is intended that these research objectives will help with generating and promulgating recommendations which will strengthen the existing legislative e-crime landscape and result in cybercrime being more effectively combated in the UAE.

1.4 Structure of the Thesis

The structure of the thesis is as follows:

Chapter One introduces the research topic and its significance to the literature on e-crime legislation. It explains the scope of the research, the research aim and objectives and provides an overview of the theoretical context of the thesis. Previous research about cyber criminology and relevant social science literature, cybercrime laws, surveillance and data retention laws in the UAE, UK and EU are investigated, as well as UK evidence law rules dealing with admissibility of electronic evidence in criminal court proceedings in order to prosecute cyber criminals.

Chapter Two is the Methodology. It presents the ontology, epistemology, philosophy, design, strategy and choices which undergird the research project. As a mixed method research approach has been chosen, this chapter makes recourse to doctrinal legal analysis/the black letter law approach, the comparative method and empirical research. It explains why the positivist approach was chosen to supplement the interpretative

stance in the form of a qualitative segment (interviews with different stakeholders). Furthermore, the chapter discusses how sensitive issues were addressed and ethics were maintained throughout the research process. Additionally, it describes how participant observation was conducted, the qualitative interviewing technique and the type of sampling, which were used. Moreover, the setting which was chosen for the interviews is outlined, as well as the method of recording and how data quality was achieved. It is also explicated how the data was analysed and why the research findings are said to be reliable and valid.

Chapter Three explores the literature and commences with an examination of the UK Computer Misuse Act 1990, as well as other relevant legislation and case law. Thereafter, the topics of interception, surveillance, communications data acquisition and decryption are discussed in the context of the UK Regulation of Investigatory Powers Act 2000 (RIPA). RIPA is analysed since this Act empowers many enforcement agencies *"to intercept communications [and] to acquire existing communications data (data held as a result of data retention...) to perform surveillance, and to demand encryption keys"*, though brief recourse is also be made to UK government programmes.[43] Subsequently, the EU and UK approach towards data retention is analysed, including the now defunct EU Data Retention Directive, as well as the (temporary and now expired) UK Data Retention and Investigatory Powers Act 2014 and the Investigatory Powers Act 2016. Thereafter, relevant UK evidence law rules,

[43] P. Bernal, *Internet Privacy Rights: Rights to Protect Autonomy* (Cambridge University Press 2014) 104-105

which deal with admissibility of intercepted communication in court proceedings, are considered.

Chapter Four investigates the legislative framework, which the UAE has adopted to combat e-crime. Recourse is made, for instance, to Federal Law No.2 of 2006 on combating cybercrime; Law No. 5 of 2012 Concerning Combating Information Technology Crimes and Law No. 3 of 2012 on Establishing the National Electronic Security Authority. It is scrutinised how these laws achieve that the digital space is being secured in the UAE. The extent to which these laws equip enforcement agencies with the power to collect information is analysed. The circumstances in which electronic information can be used as electronic evidence criminal prosecutions is critically evaluated. Recourse is made to reported e-crime cases. The existing legislative gaps are critically investigated.

Chapter Five analyses interviews with five senior experts in the field of cyber-crime. Namely: from the judiciary, the police, Interpol, the office of prosecution and the Telecommunications Regulatory Authority. Their experiences and views are critically presented, as well as their suggestions and recommendations for improvement.

Chapters Six reviews the theoretical and empirical chapters to formulate a new legal framework for the UAE. Chapter Six considers surveillance, privacy, data protection, security, the existing federal laws, the criminal procedure law and procedural laws governing electronic evidence in the UAE to see how these can be overhauled. Also

this chapter review, evaluate, distil and amend some of the primary areas of law that need to be addressed in tackling e-crime based on the black-letter law analysis and the comparative findings, as well as the practical suggestions from the interviews.

1.5 Defining Cybercrime

In the context of this thesis the term 'cybercrime' has a wider meaning, as it includes network assisted crimes, which essentially means crimes committed in the real world which have been facilitated by the use of internet/cyberspace. David Wall (2007) argues that maybe the term 'cybercrime' has been misused, arguing that the term 'cyberspace crime' may have been a better fit. Wall contends that:

"*the term has greater meaning if we construct it in terms of the transformation of criminal or harmful behaviour by networked technology, rather than simply the behaviour itself…the words cyber and crime actually sit well together linguistically. This linkage becomes more significant if we understand cybercrimes as crimes which are mediated by networked technology and not just computer*[44]*.*"

Sah and Vinent (2013) observe that whilst the internet is a great tool to develop and create, it also has the ability to damage and disrupt, especially since the world has

[44] D. Wall, *Cybercrime: The Transformation of Crime in the Information Age,* (Polity Press, 2007).

become very dependent on information technology (IT) and as a result, is an interesting space for crime.[45] As the internet has become a global communication medium for the private and public sector, extremely sensitive data is being transmitted and this has made it prone to security violations committed by, amongst others, criminals.[46]Thomas and Loader (2003) state that *"[c]ybercrime can be regarded as computer-mediated activities which are either illegal or considered illicit by certain parties and which can be conducted through global electronic networks"* [47] According to the European Commission, the terms *"cybercrime"*, *"computer-related crime"*, *"computer crime"* and *"high tech crime"* can be employed interchangeably.[48] Lestrade DATE notes that cybercrime has become widely understood to denote the phenomenon of unauthorised or criminal acts, which are perpetrated remotely due to the availability of internet technology.[49]

As noted by Goldsmith (2013), computer systems are extremely complex and this can cause malfunctions and result in vulnerabilities which can be exploited by cyber criminals in any number of ways.[50] *"The aggressor has to find only one crucial*

[45] N. Sah, V. Vinent, Cyber attack = armed attack? The implications and the challenges, 19(8) *Computer and Telecommunications Law Review* 2013, 226-233, 226

[46] E. Lestrade, The cybercrime phenomenon and Latvian cybercrime law, *European Newsletter* 2006, 1-5, 1

[47] D. Thomas, B. Loader, *Cybercrime: Law Enforcement, Security and Surveillance in the Information Age* (London, Routledge 2000) 3; cited from N. Jarvie, Control of cybercrime - is an end to our privacy on the Internet a price worth paying? Part 1, 9(3) *Computer and Telecommunications Law Review* 2003, 76-81, 78

[48] Communication from Commission to European Parliament: 2000, Creating a Safer Information Society by combating Computer-related Crime <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52000DC0890> accessed 20th January 2015; N. Jarvie, Control of cybercrime - is an end to our privacy on the Internet a price worth paying? Part 1, 9(3) *Computer and Telecommunications Law Review* 2003, 76-81, 77-78

[49] E. Lestrade, The cybercrime phenomenon and Latvian cybercrime law, *European Newsletter* 2006, 1-5, 1

[50] Jack Goldsmith, How cyber changes the laws of war, 24(1) *European Journal of International Law* 2013, 129-138, 130

weakness; the defender has to find all of them and in advance".[51] For instance, malware can be installed on a user's electronic device without this being known and can then be used for criminal purposes.[52] Cyber attacks can be launched to pursue criminal objectives, for instance, to steal information and transfer money, to extort money for unlocking infected computers, to sabotage important infrastructure, to illegally exert pressure, e.g. to tarnish the reputation of a company, to spy or illegally gather information and often these cyber attacks are perpetrated by organised crime and millions of computers can be compromised, as happened in March 2009 when malicious software was used to generate botnets,[53] which infected computers in over 100 countries and gathered sensitive information.[54] Moreover, Brannan points out that social networking sites, such as Twitter and Facebook, can be used for sexual predation and child grooming, cyber-harassment, bullying and stalking, to send threatening messages or to incite social unrest.[55]

MacEwan highlights that deception-based crime is common within cyberspace. Phising is a common form of deception to perpetrate internet fraud, it occurs when individuals are encouraged to provide private data.[56] The Anti-Phishing Working Group defines phising as *"a criminal mechanism employing both social engineering and technical*

[51] H. Kahn, E. Jones, *On Thermonuclear War* (London, Transaction Publishers 2007) 535; cited from Jack Goldsmith, How cyber changes the laws of war, 24(1) *European Journal of International Law* 2013, 129-138, 130-131
[52] Ibid (Goldsmith) 131
[53] A botnet is a robot network: N. MacEwan, A tricky situation: deception in cyberspace, 77(5) *Journal of Criminal Law* 2013, 417-432, 419
[54] EU Focus 2010, Commission proposes boosting Europe's defences against cyber-attacks, 277, 22-23, 22
[55] J. Brannan, Crime and social networking sites, 1 *Juridical Review* 2013, 41-51, 41
[56] N. MacEwan, A tricky situation: deception in cyberspace, 77(5) *Journal of Criminal Law* 2013, 417-432, 418

subterfuge."[57] Very often malware is installed in form of a Trojan, i.e. the threat goes unnoticed by the anti-virus software of the electronic device and malware becomes installed, for instance, by the user clicking on a website or a link, which results in the malware being downloaded and the device becoming infected and spyware being installed.[58]Digital extortion may occur in these circumstances, in 2013, Europol closed down a criminal network which was distributing malware on users' computers, it generated a pop-up window with the message that the computer had been locked and stated that images about sexual abuse were on the computer and that it would only be unlocked if a fine was paid.[59] It is not just computers that are vulnerable, but other digital devices and smartphones have become targets for cybercrime attacks. [60] Additionally, the webpages of companies or organisations may be targeted by cyber criminals who send them a Distributed Denial of Service (DDoS) attack to shut down their webpage using botnets (a robot network), attacks such as these can be used to steal sensitive data or Intellectual Property (IP).[61] Sensitive information can also be stolen by hackers who are able to gain unauthorised access by bypassing or circumventing the security mechanisms of a network or information system.[62] Moreover, cyber criminals

[57] Anti-Phishing Working Group (APWG), Phishing Activity Trends Report, 2nd Quarter 2012, 2, available at http://www.apwg.org/resources/apwg-reports/, accessed 13 August 2013; N. MacEwan, A tricky situation: deception in cyberspace, 77(5) *Journal of Criminal Law* 2013, 417-432, 419
[58] N. MacEwan, A tricky situation: deception in cyberspace, 77(5) *Journal of Criminal Law* 2013, 417-432, 420
[59] R. Ferguson, Police hold 11 over ransomware scam "affecting thousands, BBC News, 14 February 2013, <http://www.bbc.co.uk/news/technology-21457743> accessed 23 January 2015; N. MacEwan, A tricky situation: deception in cyberspace, 77(5) Journal of Criminal Law 2013, 417-432, 420
[60] N. MacEwan, A tricky situation: deception in cyberspace, 77(5) Journal of Criminal Law 2013, 417-432, 423
[61] Ibid, 424-425
[62] A. Nehaluddin, Hackers' criminal behaviour and laws related to hacking, 15(7) Computer and Telecommunications Law Review 2009, 159-165, 159

can employ viruses, which attack or destroy the system, or worms that can impair the system or overload it.[63] In short, cybercrime takes a multitude of diverse forms.

Longo (2013) writes that cybercrimes can be divided into three groups. Firstly, crimes which are directed against a particular computer or a network infrastructure or a particular part in order to change, destroy, harm or steal data or equipment; secondly, crimes which are directed against organisations or persons and for this purpose their computer networks or computers are targeted, for instance, cybercrimes, such as identity theft or credit card fraud; and thirdly, crimes which are committed through data which is being stored, exchanged or generated and an example is child pornography.[64] Longo (2013) describes the distinction between cybercrime and crime as *"virtually seamless."*[65] Furthermore, Lestrade characterises certain distinct features that are intrinsic to the cybercrime phenomenon: new forms of crime emerge as a result of the internet, criminal offences are perpetrated in a new venue, i.e. in cyberspace which has no borders and where criminals can be far from their victims, the mere availability of a network that enables criminals to perpetrate cybercrimes, and resultantly new legal, technical and procedural measures which have to be adopted to combat it.[66]

Rahman et al (2009) concur that existing laws are insufficient to police the vast digital world which are exacerbated by its sovereignless nature.[67] Equally, traditional forms of policing are incapable of dealing with cybercrimes, for instance, community-oriented

---

[63] Ibid, 164

[64] B. Longo, Learning on the wires: BYOD, embedded systems, wireless technologies and cybercrime, 13(2) *Legal Information Management* 2013, 119-123, 121

[65] Ibid

[66] E. Lestrade, The cybercrime phenomenon and Latvian cybercrime law, *European Newsletter* 2006, 1-5, 1

[67] M. M. Rahman, M. A. Khan, N. Mohammad, M. O. Rahman, Cyberspace claiming new dynamism in the jurisprudential philosophy: a substantive analysis of conceptual and institutional innovation, *International Journal of Law & Management* 2009, 274-289, 288

policing strategies are ineffective in catching cyber criminals, particularly since criminals can often remain anonymous when committing crimes and criminals can be based in different countries around the world.[68] Walker et al (2006) highlight that when cybercrime is committed there are more invisible venues than visible venues and that there is also more faceless crime making investigation and prosecution much more difficult.[69] In cyberspace computers are globally linked which makes it harder for law enforcement agents to deter individuals from committing cybercrimes. A central issue is that domestic law enforcement agencies rely on their counterparts in other countries who may be slow to cooperate, this is turn makes it easier for cyber criminals to avoid prosecution, and even in cases where cooperation is forthcoming, investigating cybercrime is resource-intensive and in other cases it simply is not possible to identify cyber criminals with sufficient certainty due to the anonymity which exists within the virtual realm.[70]

McCusker (2003) suggests that the inherently global nature of the internet requires international regulation, as opposed to national regulation, but points out that this has not yet been fully achieved.[71] In 1990, the United Nations passed a resolution about computer crime legislation in Havana during a Congress about the Prevention of Crime and the Treatment of Offenders, and in 1994, the United Nations Manual on the Prevention of Computer-related Crime was prepared, however, Rychlicki (2006) notes

[68] D. Walker, D. Brock, T. R. Stuart, Faceless-orientated policing: traditional policing theories are not adequate in a cyber world, *Police Journal* 2006, 169-176, 169
[69] Ibid, 175
[70] Jack Goldsmith, How cyber changes the laws of war, 24(1) *European Journal of International Law* 2013, 129-138, 131-132
[71] R. McCusker, E-commerce, business and crime: inextricably linked, diametrically opposed? 23(1) *Company Lawyer* 2002, 3-8, 6

that this has not been revised and is no longer up to date due to rapid technological advances.[72] Similarly, the UN recognises that *"[l]aws, criminal justice systems and international co-operation have not kept pace with technological change. Only a few countries have adequate laws to address the problem, and of these, not one has resolved all of the legal, enforcement and prevention problems."*[73] Nevertheless, the International Criminal Police Organisation (Interpol) renders assistance and co-operates with law enforcement officers from around the world and included in its remit are IT crimes.[74] Rychlicki (2006), explicates that Interpol hosts a convention entitled the European Working Party on Information Technology Crime and at this convention, the Information Technology Crime Investigation Manual was produced.[75]

Respecting this international context, the Council of Europe Convention on Cybercrime 2001 was adopted by several countries. Carr and Williams (2001) explain that the Convention distinguishes four types of offences:

1. Those which contravene confidentiality and affect the availability and integrity of computer systems and data.
2. Computer-related crimes, such as computer fraud.
3. Copyright offences.
4. Content offences, such as child pornography.

---

[72] T. Rychlicki, Legal issues of criminal acts committed via botnets, 12(5) *Computer and Telecommunications Law Review* 2006, 161-167, 164

[73] International Review of Criminal Policy, United Nations Manual on the Prevention and Control of Computer-Related Crime, Nos.43-44 , 1999 <http://www.uncjin.org/Documents/irpc4344.pdf> accessed 20th January 2015; cited from R. McCusker, E-commerce, business and crime: inextricably linked, diametrically opposed? 23(1) *Company Lawyer* 2002, 3-8, 6

[74] T. Rychlicki, Legal issues of criminal acts committed via botnets, 12(5) *Computer and Telecommunications Law Review* 2006, 161-167, 164

[75] Ibid

The penalties for the above offences are left to the state parties to determine.[76] Liability can also be imposed on legal entities, such as corporations, when they benefit from the commission of an offence, but only when the action is attributable to key personnel.[77] Jerome (2012) explains that the Convention does not obligate state parties to provide mutual assistance when this contravenes the national law of the state party, or when the state deems that the request contravenes its security, sovereignty, public order or other important national interests.[78] Extradition of a cyber criminal who is a national of the requested state may be refused if the state has domestic laws in place to punish the person for the offences stipulated in the Convention, or where the request contravenes the national laws and reservations can be entered to the Convention.[79] A drawback is that these caveats could undermine the overall effectiveness of the Convention.

The failure to adopt any other international treaty and the difficulties in combating cybercrime at the domestic level highlight, as Gersch (2012) observes, *"the law['s] struggle to keep up with the pace of technical innovation."*[80] Cybercrime is a unique, unorthodox and extraordinary phenomenon which raises the question as to whether

[76] I. Carr, K. S. Williams, Cyber-crime and the Council of Europe: reflections on a Draft Convention, 7(4) *International Trade Law & Regulation* 2001, 93-96, 94
[77] Ibid
[78] Articles 27(3) and (4)(b) and 29(5)(b) of the Council of Europe Convention on Cybercrime 2001; O. U. Jerome, Russia and the Council of Europe Convention on Cybercrime, 18(1) *Computer and Telecommunications Law Review* 2012, 16-17, 16
[79] Article 22(3) and Articles 4(2), 6(3)9(4), 10(3), 11(3), 14(3), 22(2), 29(4), 41 and 42 of the Council of Europe Convention on Cybercrime 2001; ibid (Jerome) 16
[80] A. Gersch, Covert surveillance - a snoopers' charter? *Archbold Review* 2012, 5-8, 5

traditional criminological theories which deal with physical crimes can be extended to the digital realm,[81]this is the focus of the next section.

1.6 The Theoretical Context of and Applicable Social Science Literature on Cybercrime

The World Wide Web and computers have become an integral aspect of modern human life. They are used in multiple modes of communications, commerce, and government, but the technological innovation which has given rise to the e-revolution has equally created new opportunities for deviant behaviour.[82] Criminological studies have been conducted in order to explain different types of cybercrimes and to test to what extent conventional theories can be applied to the digital age.[83]

Classical criminology considers that persons commit crime after weighing up the benefits and costs i.e. that crime is the consequence of a rational and calculated decision.[84] It is therefore important that people are deterred from committing crimes and this requires severe and prompt punishment.[85] The positivist school within criminology points out that crime is caused by psychological, biological and social factors, which persons cannot control and therefore does not favour punishment, but that instead the

[81] M. Yar, The Novelty of 'Cybercrime', An Assessment in Light of Routine Activity Theory, 2(4) *European Journal of Criminology* 2005, 407-427, 407
[82] T. J. Holt, A. M. Bossler, An Assessment of the Current State of Cybercrime Scholarship, 35(1) *Deviant Behavior* 2014, 20-40, 20
[83] Ibid
[84] G. F. Vito, J. R. Maahs, R. M. Holmes, *Criminology: Theory, Research, and Policy* (2nd ed, Sudbury, Jones and Bartlett Publishers 2007) 15
[85] Ibid

factors which caused the crime are *"treated"* and therefore focuses on rehabilitation.[86] However, this school has largely become replaced by the neoclassical school which focuses on the person, choice and individual responsibility.[87] With the advent of the digital age, countries adopted cybercrime legislation in order to send out a clear message that these types of crime result in punishment in line with the classical and neo-classical school of thought.[88] The neo-classical school of thought advocates a deterrence model, but in comparison to the classical school of thought the neo-classical school also considered the circumstances of the person or the particular situation in order to impose a stricter or more lenient sentence.[89]

However, this is not the only theoretical view. Gottfredson and Hirschi (1990) explain that the "*motive to crime is inherent or limited to immediate gains provided by the act itself"* and *"there is no larger purpose behind...theft, or insider trading"* and thus espouse a *"general theory of crime."*[90] Certain characteristics, such as inability to self-control, can result in impulsive behaviour since immediate benefits are thereby reached without reflection about the consequences and risks.[91] This may render individuals more vulnerable and expose them to offender groups, thereby increasing the chance of

[86] Ibid
[87] J. M. Miller, *The Encyclopedia of Theoretical Criminology* (London, Wiley Blackwell 2014) 261
[88] R. G. Smith, P. Grabosky, G. Urbas,*Cyber Criminals on Trial* (Cambridge, Cambridge University Press 2004) 86
[89] S. G. Tibbetts, C. Hemmens, *Criminological Theory: A Text/Reader* (London, SAGE 2010) 66
[90] M. R. Gottfredson, T. Hirsch, *A General Theory of Crime* (Stanford, Stanford University Press 1990) 256; E. Goode, *Out of Control: Assessing the General Theory of Crime* (Stanford, Stanford University Press 2008) 214
[91] C. Cunha, M. Manuela, *Handbook of Research on Digital Crime, Cyberspace Security, and Information Assurance* (Hershey, Information Science Reference 2015) 219

victimisation.[92] Empirical studies have also established that limited individual self-control can be linked to particular types of cybercrime and this includes software piracy,[93] illicit music downloads and online pornography.[94] Yet it may also be argued that young people often do not consider that their behaviour is criminal, the act can be done with ease and because they consider it unlikely that they will be caught. Another study supports Gottfredson and Hirschi's theory i.e. that a lack of self-control increases the chances of cyber stalking, since persons who lack self-control are not strong enough to resist participating in such behaviour and are unable to appreciate the consequences which flow from this.[95] Nonetheless, whilst this argument appears more convincing with illegal downloads, it is not as persuasive in relation to cyberstalking where it is unlikely that this is the only motivator in this case. However, an empirical study which tested whether self-control could account for different types of cybercrime victimisation found that there was no direct link i.e. the loss of digital data as a result of malware infection or the theft of banking passwords had no correlation to any discrete characteristics or choices of a victim.[96] Victims of cybercrime are very rarely at fault, though low computer literacy might be viewed as a contributing factor. Computers can become infected by viruses without any communication between the perpetrator and the

[92] T. Buzzel, D. Foss, Z. Middleton, Explaining use of online pornography: A test of self-control theory and opportunities for deviance, 13 *Journal of Criminal Justice and Popular Culture* 2006, 96-116, 96
[93] G. E. Higgins, Can low self-control help with the understanding of the software piracy problem? 26 *Deviant Behavior* 2006, 2005, 1-24, 1
[94] G. E. Higgins, S. E. Wolfe, C. D. Marcum, Digital piracy: An examination of three measurements of self-control, 29 *Deviant Behavior* 2008, 440-460, 440
[95] C. D. Marcum, G. E. Higgins, M. L. Ricketts, Juveniles and Cyber Stalking in the United States: An Analysis of Theoretical Predictors of Patterns of Online Perpetration, 8(1) *International Journal of Cyber Criminology* 2014, 47-56, 53
[96] A. M. Bossler, T. J Hold, The effect of self-control on victimization in the cyberworld, 38(3) *Journal of Criminal Justice* 2010, 227-236, 233

victim.[97] It was established that self-control was only relevant when a particular person was targeted.[98] Other studies have produced mixed findings about the link between computer hacking and a lack of self-control, thereby not fully endorsing this general theory of crime.[99] Moreover, critics say that crime cannot be reduced to one factor in this way.[100]

Akers advocates a *"social learning theory"* and explains that individuals can choose to learn or to unlearn certain acts and this includes learning/unlearning restrains.[101] This theory posits that persons adopt deviant behaviour and opt for a criminal career because their particular learning process exposes them to various associations, for instance, peers engage in deviant behaviour[102], these deviant behaviour patterns are imitated and then there is reinforcement of such behaviour, e.g. in the form of prospective benefits and disadvantages.[103] Social learning is very relevant to cybercrime since the perpetrator has to learn technical skills and procedures to use the computer illicitly.[104] Research confirms that three constitutive aspects of social learning theory can be found in respect to cybercrime:

---

[97] Ibid
[98]Ibid, 234
[99] A. M. Bossler, G. W. Burruss, 'The general theory of crime and computer hacking: Low self-control hackers?' in (eds) T. J. Holt, B. Schell, *Corporate hacking and technology-driven crime: Social dynamics and implications* (Hershey, IGI Global 2010) 57-81, 57
[100] G. D. Walters, *Criminal Belief Systems: An Integrated-Interactive Theory of Lifestyles: An Integrated-Interactive Theory of Lifestyles* (Westport, Praeger Publishers 2002) 197
[101] See R. L. Akers, (Boston, Northeastern University Press 1998); C. L. Britt, M. R. Gottfredson, *Control Theories of Crime and Delinquency* (New Brunswick, Transaction Publishers 2003) 42
[102] R. L. Akers, G. Lee, A longitudinal test of social learning theory: Adolescent smoking, 26 *Journal of Drug Issues* 1996, 317-343, 317
[103] S. Boeringer, C. L. Shehan, R. L. Akers, Social contexts and sexual learning in sexual coercion and aggression: Assessing the contribution of fraternity membership, 40 *Family Relations* 1991, 558-564, 558; T. J. Holt, A. M. Bossler, D. C. May, Low self-control, deviant peer associations, and juvenile cyberdeviance, 37(3) *American Journal of Criminal Justice* 2012, 378-395, 381
[104] W. F. Skinner, A. M. Fream, A social learning theory analysis of computer crime among college students, 34 *Journal of Research in Crime and Delinquency* 1997, 495-518, 498

1. People prefer that laws are violated which govern how computers and the internet are used.[105]
2. There exist illegal computer models which they can copy.[106]
3. They are encouraged to breach computer laws.[107]

Research also found that those who socialise with deviant groups are more prone to cyber stalk others, thereby confirming Akers' theory.[108] Another study points out that self-control is not as critical when compared to having peers who engage in deviant behaviour.[109] Hence, in the context of cyber-stalking, the social learning theory and lack of self-control have been linked.[110] Individuals who regularly associate with deviant peers and find it hard to control their impulses were more prone to cyber stalk other juveniles.[111]

Furthermore, empirical research highlights that the same risk factors which are present when online victimisation occurs also exist in respect of hacking.[112] A lack of self-

[105] R. G. Morris, G. E. Higgins, Criminological theory in the digital age: The case of social learning theory and digital piracy, 38 *Journal of Criminal Justice* 2010, 470-480, 470
[106] T. J. Holt, G. W. Burruss, A. M. Bossler, Social learning and cyber deviance: Examining the importance of a full social learning model in the virtual world, 33(2) *Journal of Crime and Justice* 2010, 31-61, 31
[107] S. Hinduja, J. W. Patchin, Cyberbullying: An exploratory analysis of factors related to offending and victimization, 29 *Deviant Behavior* 2008, 129-156, 129
[108] C. D. Marcum, G. E. Higgins, M. L. Ricketts, Juveniles and Cyber Stalking in the United States: An Analysis of Theoretical Predictors of Patterns of Online Perpetration, 8(1) *International Journal of Cyber Criminology* 2014, 47-56, 53
[109] T. J. Holt, A. M. Bossler, D. C. May, Low self-control, deviant peer associations, and juvenile cyberdeviance, 37(3) *American Journal of Criminal Justice* 2012, 378-395, 392
[110] C. D. Marcum, G. E. Higgins, M. L. Ricketts, Juveniles and Cyber Stalking in the United States: An Analysis of Theoretical Predictors of Patterns of Online Perpetration, 8(1) *International Journal of Cyber Criminology* 2014, 47-56, 53
[111] Marcum et al (ibid) 49&53
[112] J. Van Wilsem, Hacking and Harassment—Do They Have Something in Common? Comparing Risk Factors for Online Victimization, 29(4) *Journal of Contemporary Criminal Justice* 2013, 437-453, 437

control was found to lead to a higher probability of both online harassment and hacking, though a person's online behaviour was thought to carry certain consequences, for instance, regular social media use increased the chance of online harassment.[113]

The occurrence of crime can also be explained through the lens of cultural deviance theory, which focuses on the practices, assumptions, beliefs and values of societies and sub-groups which encourage deviant conduct and this is linked to social learning theory i.e. social learning can be influenced by cultural deviance.[114] The sub-cultural and social learning approaches thus argue that groups have the same values and this can be applied in the virtual realm, particularly to hackers who often learn their skills from peers.[115] Computer-aided communications and the internet can thus promote the creation of illegal subcultures.[116] For instance, subcultures of computer hacking and malware writing have emerged.[117] It was found that the majority of these hackers were young men who were members of a culture which promoted the sharing of information, skills and beliefs; they were often graduates who were extremely skilled and regularly networked with each other.[118] Moreover, empirical research has found that online subcultures of sexual deviants have emerged.[119] Hence, the internet allows people with deviant interests to connect and engage in deviant behaviour.

---

[113] Ibid
[114] M. Inderbitzin, K. A. Bates, R. Gainey, *Deviance and Social Control: A Sociological Perspective* (London, SAGE Publications Inc 2013) 244
[115] J. M. Miller, *The Encyclopedia of Theoretical Criminology* (London, Wiley Blackwell 2014) 748
[116]K. R. Blevins, T. J. Holt, Examining the virtual subculture of johns, 38(5) *Journal of Contemporary Ethnography* 2009, 619-648, 638
[117] T. J. Holt, D. Strumsky, O. Smirnova, M. Kilger, Examining the social networks of malware writers and hackers, 6(1) *International Journal of Cyber Criminology* 2012, 891-903, 891 & 901
[118] Ibid, 901
[119] K. R. Blevins, T. J. Holt, Examining the virtual subculture of johns, 38(5) *Journal of Contemporary Ethnography* 2009, 619-648, 619

A similar theory to cultural deviance theory is social disorganisation theory, which considers that geographical places and social control are related to crime.[120] This perspective has also become known as the Chicago School.[121] This is because the initial advocates - Shaw and McKay (1942) – promulgated this model by studying the rates of juvenile arrests in Chicago.[122] Shaw and McKay employed Park, Burgess and McKenzie's (1925) concentric zone model which divided Chicago into five different zones, commencing with the city centre and ending with the outer boundaries.[123] They found that crime decreased the further the location was away from the centre, irrespective of the type of neighbourhood or ethnic group which lived there, though in certain transitioning areas crime rates were continuously high.[124] The results suggested that delinquency rates in city areas were linked to poverty, a diverse ethnic spread and instability within the community.[125] Shaw and McKay (1942) contend that social disorganisation is at the heart of delinquency; it is the result of a deficiency of mutual values, inadequate social control within the community and is influenced by the location

[120] G. F. Vito, J. R. Maahs, R. M. Holmes, C*riminology: Theory, Research, and Policy* (2nd ed, London, Jones and Bartlett Publishers 2007) 177
[121] M. DeLisi, K. M. Beaver, *Criminological Theory: A Life-Course Approach* (London, Jones and Bartlett Publishers International 2011) 136
[122] Also see C. R. Shaw, H. D. McKay, *Juvenile Delinquency in Urban Areas* (Chicago, University of Chicago Press 1942); M. DeLisi, K. M. Beaver, *Criminological Theory: A Life-Course Approach* (London, Jones and Bartlett Publishers International 2011) 136
[123] R. E. Park, E. W. Burgess, R. D. McKenzie, *The city* (Chicago, The University of Chicago Press 1925); M. DeLisi, K. M. Beaver, *Criminological Theory: A Life-Course Approach* (London, Jones and Bartlett Publishers International 2011) 135
[124] Also see C. R. Shaw, H. D. McKay, *Juvenile Delinquency in Urban Areas* (Chicago, University of Chicago Press 1942); M. DeLisi, K. M. Beaver, *Criminological Theory: A Life-Course Approach* (London, Jones and Bartlett Publishers International 2011) 135
[125] Also see C. R. Shaw, H. D. McKay, *Juvenile Delinquency in Urban Areas* (Chicago, University of Chicago Press 1942); M. DeLisi, K. M. Beaver, *Criminological Theory: A Life-Course Approach* (London, Jones and Bartlett Publishers International 2011) 135

and neighbourhood, as opposed to individual characteristics.[126] The core argument of this theory is that disordered and fragile communities are more prone to higher crime rates since their members become connected to their environment and positively link this with their commitment to combating crime.[127] In sum, the characteristics of a neighbourhood have an impact on the crime rate.[128] In the context of cybercrime, this theory suggests that steps should be taken to develop a strong attachment amongst the online community in order to combat cybercrime, and there are websites which do this, they are regularly visited and are used for the exchange of opinions, and to tag and rate posts, utilising these communities could be an effective strategy in fighting cybercrime.[129] However, even strong networks can become deviant or develop deviancy.

Another important theory, which is a derivative of the previous theory, is situational crime prevention theory.[130] Clarke (1980) points out that individuals are being motivated to commit crime by a mixture of immediately arising situational factors, which fit the particular characteristics of the person's past and aspects which match the present situation of the person.[131] Accordingly, proponents of situational crime prevention theory argue that a systematic eradication of opportunities to commit crime substantially

[126] Ibid (DeLisi and Beaver) 135-136
[127] N. Kshetri, *The Global Cybercrime Industry: Economic, Institutional and Strategic Perspectives* (London, Springer-Verlag 2010) 232
[128] G. F. Vito, J. R. Maahs, R. M. Holmes, C*riminology: Theory, Research, and Policy* (2nd ed, London, Jones and Bartlett Publishers 2007) 177
[129] N. Kshetri, *The Global Cybercrime Industry: Economic, Institutional and Strategic Perspectives* (London, Springer-Verlag 2010) 232
[130] R. M. Bohm, B. Vogel, *A Primer on Crime and Delinquency Theory* (3rd ed, Belmont, Wadsworth Cengage Learning 2011) 76
[131] R. V. G. Clarke, Situational Crime Prevention: Theory and practice, 20(2) *British Journal of Criminology* 1980, 136-147, 136; M. H. Tonry, *The Handbook of Crime & Punishment* (Oxford, Oxford University Press 1998) 372

reduces the overall crime rate.[132] However, so long as criminal motivation is not also diminished, this view may be challenged and it is therefore best to perceive crime as the result of interplay between opportunity and motivation.[133] It has therefore been argued that cybercrime arises because the internet affords anonymity and therefore has a disinhibition effect.[134] This may also explain the occurrence of cyber stalking. This theory is thus insightful in the context of cybercrime since it emphasises the importance of defending targets, for instance, through the use of safe passwords.[135]

A similar theory is opportunity theory because situational crime prevention depends on opportunity.[136] An opportunity arises and individuals feel more empowered to misbehave due to the *"dissociative anonymity"* which the internet offers.[137] Mayhew et al (1973) point out that opportunities can be described in many different ways and therefore distinguish between opportunities which relate to persons, for instance, the chance to be victimised, and opportunities which depend on objects, for instance, the security of the item, the degree of surveillance, the attractiveness of the item and opportunities can therefore depend on a multitude of factors which determine how much risk, effort will be expended.[138] Opportunity theory employs a *"rational choice theory for offending"* because it is assumed that perpetrators weigh up possible gains against

[132] R. V. Clarke, 'Situational Prevention' in (eds) A. Von Hirsch, D. Garland, A. Wakefield, *Ethical and Social Perspectives on Situational Crime Prevention* (Oxford, Hart Publishing 2002) 97
[133] Ibid
[134] J. Suler, 'The Online Disinhibition Effect' (2004) 7(3) *Cyberpsychology & Behaviour*, 321-325, 321
[135] S. Bryant, R. Bryant, *Policing Digital Crime* (Farnham, Ashgate Publishing Ltd 2014) 65
[136] M. H. Tonry, *The Handbook of Crime & Punishment* (Oxford, Oxford University Press 1998) 372
[137] J. Suler, 'The Online Disinhibition Effect' (2004) 7(3) *Cyberpsychology & Behaviour*, 321-325, 322&324
[138] See P. Mayhew, R. V. Clarke, M. Hough, A. Sturman, Crime as Opportunity, Home Office Research Study No.34 (London, HMSO 1973); M. H. Tonry, *The Handbook of Crime & Punishment* (Oxford, Oxford University Press 1998) 372-373

detriments and this perspective is implicitly accepted by situational crime prevention theory.[139] This theory can be perceived as a species of deterrence theory, for instance, by rendering it more difficult for online criminals to launch phishing attacks, the cost-benefit assessment shifts and results in criminals becoming deterred.[140]

Another derivative of the Chicago School is Felson and Cohen's (1979) *"routine activities theory"* which holds that property or personal crimes take place when there is a criminal who perpetrates a crime, an item of property or a victim and the situation and other individuals facilitate the crime or someone else or the victim is present and who can take steps to avert the crime.[141] These constituent characteristics of place, time, persons and objects are divided into the following three core groups of variables: firstly, offenders who are motivated; secondly, appropriate targets which can be criminally victimised; and thirdly, guardians who are incapable of protecting the property or persons.[142] The core tenet is thus that criminal victimisation increases when *"space and time of the three minimal elements of direct-contact predatory violations"* converge.[143] This theory has been expanded to cover white-collar crime and illicit drug dealing by pointing out that these crimes are made possible when a criminal is motivated, has

[139] R. Reiner, *The Oxford Handbook of Criminology* (4th ed, Oxford, Oxford University Press 2007) 541
[140] S. Bryant, R. Bryant, *Policing Digital Crime* (Farnham, Ashgate Publishing Ltd 2014) 65

[141] L. Cohen, M. Felson, Social Change and Crime Rate Trends: A Routine Activity Approach, 44(4) *American Sociological Review* 1979, 588–608, 588; R. L. Akers, *Criminological Theories: Introduction and Evaluation* (Abingdon, Routledge 2013) 27; R. M. Bohm, B. Vogel, *A Primer on Crime and Delinquency Theory* (3rd ed, Belmont, Wadsworth Cengage Learning 2011) 76
[142] L. Cohen, M. Felson, Social Change and Crime Rate Trends: A Routine Activity Approach, 44(4) *American Sociological Review* 1979, 588–608, 588; R. L. Akers, *Criminological Theories: Introduction and Evaluation* (Abingdon, Routledge 2013) 27
[143] L. Cohen, M. Felson, Social Change and Crime Rate Trends: A Routine Activity Approach, 44(4) *American Sociological Review* 1979, 588–608, 589

located an adequate target and there is no effective guardianship.[144] For a target to be suitable, it must have a value and it is not too difficult to move the object, the object is visible and it is easy to gain access.[145] A cyber criminological stance highlights the usefulness of this theory; particularly in the context of hackers trying to create botnets i.e. various linked computers without their owners' knowledge, though also in respect of other cybercrimes.[146] These computers can become appropriate targets, which can be used to stage a distributed denial of service attack when there is no appropriate guardian e.g. the computer has no firewall and anti-virus software.[147]

Hindeland, Gottfredson, Garofalo (1978) developed the *"lifestyle-exposure theory"* which is based on the assumption that different lifestyles have an impact on the exposure to dangerous people, times and places and lifestyles are *"routine daily activities, both vocational activities (work, school, keeping house, etc) and leisure activities."*[148] This theory can be applied to the digital realm since online lifestyle and digitally adept guardianship can impact cybercrime victimisation.[149]

Both the routine activity theory and the lifestyle-exposure theory have been amalgamated as part of a joint *"opportunity theory of victimisation"* which assumes that

[144] G. F. Vito, J. R. Maahs, R. M. Holmes, *Criminology: Theory, Research, and Policy* (2nd ed, London, Jones and Bartlett Publishers 2007) 69
[145] G. F. Vito, J. R. Maahs, R. M. Holmes, *Criminology: Theory, Research, and Policy* (2nd ed, London, Jones and Bartlett Publishers 2007) 69
[146] G. Kirwan, *The Psychology of Cybercrime: Concepts and Principles: Concepts and Principles* (Hershey, Information Science Reference 2012) 47
[147] Ibid
[148] M. Hindelang, M. Gottfredson, J. Garofalo, *Victims of personal crime: An empirical foundation for a theory of personal victimization* (Cambridge, Ballinger 1978)
241; M. McShane, F. P. Williams, *Victims of Crime and the Victimization Process* (Abingdon, Routledge 2013) 232
[149] K. Jaishankar, *Cyber Criminology: Exploring Internet Crimes and Criminal Behavior* (Boca Raton, CRC Press 2011) 243

victimisation is caused by opportunities and certain lifestyles, and daily activities promote criminal opportunities.[150] In the context of cybercrime, the life-style exposure theory has been modified to the digital space and used to predict different kinds of victimisation, for example, cyber-stalking, virus infection or threats.[151] *"Lifestyle-routine activities theory"* may account for the occurrence of cyber and computer crime, though not many empirical tests have been conducted to verify this.[152] Yet a study by Hold and Bossler (2008), which investigated the *"lifestyle-routine activities theory"* amongst university students, supports that peer involvement can lead to individual victimisation.[153] Equally, another empirical investigation found that online harassment is endemic amongst high school students who often communicate with technologically enabled devices.[154]

This suggests that criminological theories can be applied to certain kinds of cybercrimes[155] and empirical research particularly supports the *"general theory of crime"* advocated by Gottfredson and Hirschi (1990), as well as the *"social learning theory"* espoused by Akers (1973).[156] However, the arguments underlying situational crime prevention theory and opportunity theory are also very convincing. They say that a person who commits a crime online can dissociate from anxiety and guilt - which may

[150] J. M. Miller, *The Encyclopedia of Theoretical Criminology* (London, Wiley Blackwell 2014) 219
[151] J. M. Miller, *The Encyclopedia of Theoretical Criminology* (London, Wiley Blackwell 2014) 219
[152] T. J. Holt, A. M. Bossler, Examining the Applicability of Lifestyle-Routine Activities Theory for Cybercrime Victimization, 30(1) *Deviant Behavior* 2008, 1-25, 1
[153] Ibid
[154] A. M. Bossler, T. J. Holt, D. C. May, Predicting online harassment victimization among a juvenile population, 44(4) *Youth & Society* 2012, 500-523, 500
[155] J. Van Wilsem, Hacking and Harassment—Do They Have Something in Common? Comparing Risk Factors for Online Victimization, 29(4) *Journal of Contemporary Criminal Justice* 2013, 437-453, 437
[156] T. J. Holt, A. M. Bossler, K. C. Seigfried-Spellar, *Cybercrime and Digital Forensics: An Introduction* (Abingdon, Routledge 2015) 283; T. J. Holt, A. M. Bossler, D. C. May, Low self-control, deviant peer associations, and juvenile cyberdeviance, 37(3) *American Journal of Criminal Justice* 2012, 378-395

otherwise be present - and feel safe in the anonymity that the internet affords, which in turn reduces the likelihood of their being caught. Within this context, Suler's (2004) argument that there exists an online disinhibition effect is very persuasive.[157]

The UK has adopted several measures to combat cybercrime and to secure the digital realm. Cybercrime and cyber security have become critical topics for the European legislator. Correspondingly, the UAE has taken steps to protect its citizens against this emerging threat. The subsequent sections will investigate the diverse legal strands which these jurisdictions have adopted.

1.7 Cybercrime Laws in the UK

Kelly (2007) explains that the UK adopted the Computer Misuse Act 1990,[158] to combat computer hacking, the necessity for such an enactment was highlighted on several occasions, with the most influential being the 1989 Law Commission's Report[159] and the House of Lords case *R v Gold.*[160] In the 1989 Law Commissions Report it was highlighted that the criminal law applying to computer crime had gaps in the protection offered. At that stage the Law Commission was mainly concerned with the act of hacking, noting however other issues such as the inapplicability of deception offences to computers.[161] One of the questions which troubled the Law Commission was whether the unauthorised access to a computer i.e hacking, should be made a criminal offence or

[157] J. Suler, 'The Online Disinhibition Effect' (2004) 7(3) *Cyberpsychology & Behaviour*, 321-325, 321
[158] As amended by the Police and Justice Act 2006
[159] Law Commission's Report No. 186 (Cmnd. 819) 1989.
[160] [1988] AC 1063; J. X. Kelly, Computer Misuse Overview, JISC Legal Information, 2007 <http://www.jisclegal.ac.uk/LegalAreas/ComputerMisuse/ComputerMisuseOverview.aspx> accessed 17 June 2014
[161] D. Ormerod, *Smith and Hogan's Criminal Law* (13th edn, OUP 2011).

whether civil law could offer sufficient protection and remedies. This was considered in the Law Commission Working Paper no.110, where the Law Commission reached the conclusion that civil law is essentially an ineffective remedy against unauthorised access[162], and therefore concluding that there is a strong case for creating a criminal offence for unauthorised access. This recommendation was made concrete in the Law Commission report og 1989, and was conceptualized through its encapsulation in the Computer Misuse Act 1990.

In *R v Gold*, the British telecom Prestel Gold computer network was unlawfully accessed and data was changed and one of the computer hackers even wrote a note for the Duke of Edinburgh. The accused were journalists who argued that they had only accessed the network to bring to light security vulnerabilities; they were nevertheless prosecuted by virtue of s.1 of the Forgery and Counterfeiting Act 1981 on the basis that they used a fake instrument, i.e. a fake customer identification number. However, the Court of Appeal and the House of Lords did not find them guilty since at the time it was not considered sufficient to deceive a machine. Nehaluddin (2009) explains that the decision suggested that hacking of computers did not constitute a criminal offence[163] and this lacuna in the law prompted the passing of the Computer Misuse Act 1990.

The Computer Misuse Act 1990 sets out the following three core offences: accessing the data or program on a computer without authority (s.1), facilitating this (s.2),

[162] Law Commission, Working Paper No. 110, 74.
[163] A. Nehaluddin, Hackers' criminal behaviour and laws related to hacking, 15(7) *Computer and Telecommunications Law Review* 2009, 159-165, 162; N. Jarvie, Control of cybercrime - is an end to our privacy on the Internet a price worth paying? Part 1, 9(3) *Computer and Telecommunications Law Review* 2003, 76-81, 79

intentionally impairing the computer from operating (s.3(2)(a)), hindering or preventing that data or a program can be accessed on a computer (s.3(2)(b)), impairing that the program operates or impairing that the data is reliable (s.3(2)(c)) and facilitating any of this (s.3(d)).[164]

S.1 is specifically designed to cover hacking and no intention has to be established in respect of the data or program. Yet in the widely publicised case of Paul Bedworth, the defence argued that he was an addict, who therefore undertook hacking and did not have the required *mens rea*. Nehaluddin explains that this resulted in the jury acquitting him and this caused concern that the Act was not stringent enough.[165]

S.2 covers circumstances in which access has been gained without authorisation with intention to perpetrate another offence.[166] S.3 has been enacted to criminalise situations where acts are done which result in contents being modified without authorisation with the intention to damage the data and modification encompasses adding, removing or altering data.[167] The Act applies to all, who have not been authorised to use or access data or programs.[168] In *R v Bow Street Magistrates Court ex parte Allison,*[169] it was

[164] M. Gregory, D. Glance, *Security and the Networked Society* (London, Springer 2013)
[165] A. Nehaluddin, Hackers' criminal behaviour and laws related to hacking, 15(7) *Computer and Telecommunications Law Review* 2009, 159-165, 162
[166] N. Jarvie, Control of cybercrime - is an end to our privacy on the Internet a price worth paying? Part 1, 9(3) *Computer and Telecommunications Law Review* 2003, 76-81, 79
[167] N. Jarvie, Control of cybercrime - is an end to our privacy on the Internet a price worth paying? Part 1, 9(3) *Computer and Telecommunications Law Review* 2003, 76-81, 79
[168] *R. v Bow Street Magistrates Court Ex p. Allison* [1999] 4 All ER 1; N. Jarvie, Control of cybercrime - is an end to our privacy on the Internet a price worth paying? Part 1, 9(3) *Computer and Telecommunications Law Review* 2003, 76-81, 79
[169] [1999] 4 All ER 1

confirmed that even authorised users, who are misusing facilities, can expose themselves to criminal liability.[170] Hence, the Act has a very wide scope.

Jarvie (2003) explicates that the terms data, computer or program are not defined by the Act, so that they are not limited to the understanding when the Act was passed.[171] Consequently, these can be interpreted flexibly to cover new technological innovations, such as smart-phones which are computers and this ensures that the scope of the Act is not curtailed.

Additionally, the Police and Justice Act 2006 has made various amendments to the Computer Misuse Act 1990 to deal with challenges in a rapidly changing digital landscape.[172] For example, McEwan (1990) writes that *"Denial of Service (DoS) attacks"* have become more commonplace, but that it was unclear whether they were covered by the Computer Misuse Act 1990.[173] Equally, Rychlicki (2006) points to an unreported Wimbledon Magistrates' Court case, which suggested that DoS/DDoS attacks were not covered by the Computer Misuse Act 1990 and explains that this resulted in the amendments by virtue of the Police and Justice Act 2006.[174]

McEwan (2008) opines that these amendments were a *"progressive move"* as deterrence was heightened and offences became extraditable in line with Article 6 of the European Union's Framework Decision 2005/222/JHA on attacks against information systems, as

[170] N. Jarvie, Control of cybercrime - is an end to our privacy on the Internet a price worth paying? Part 1, 9(3) *Computer and Telecommunications Law Review* 2003, 76-81, 80
[171] N. Jarvie, Control of cybercrime - is an end to our privacy on the Internet a price worth paying? Part 1, 9(3) *Computer and Telecommunications Law Review* 2003, 76-81, 79
[172] N. MacEwan, The Computer Misuse Act 1990: lessons from its past and predictions for its future, 12 Criminal Law Review 2008, 955-967, 955 and 957
[173] Ibid
[174] T. Rychlicki, Legal issues of criminal acts committed via botnets, 12(5) *Computer and Telecommunications Law Review* 2006, 161-167, 166

now replaced by the new EU Directive 2013/40 on attacks against information systems.[175] Additionally, further amendments to the Computer Misuse Act 1990 were made by virtue of the Serious Crime Act 2015.[176] The Explanatory Notes to the Serious Crime Act inform that the amendments modernise the offences, so that tools to perpetrate cybercrime, for instance, programmes with which computer systems can be unlawfully accessed, are covered.[177] Moreover, a new section 3ZA is inserted into the Computer Misuse Act 1990 to create the *"offence of impairing a computer such as to cause serious damage"*, as currently only s.3 covers this, but this section only allows a maximum penalty of up to ten years, which the government considers too lenient in serious cases, for instance, when critical infrastructure is damaged.[178] The new penalty is 14 years or life imprisonment. S.3ZA(1) spells out the criteria which have to be met to establish that the offence is made out: Firstly, for the *actus reus* to be made out the perpetrator has to commit an act without authorisation in respect of a computer which creates a substantial risk of *"serious damage"*, which is *"of a material kind"*; and secondly, the *mens rea* is established by showing that s/he knew that there was no authority and it was intended that such serious damage was caused or the person was reckless in respect of the damage.[179] An unauthorised act takes place when the person is not responsible for the computer and cannot thereby decide to do the act and the person

[175] Ibid, 959; M. Turner, N. Pantlin, L. Pugh, C. Young, EU Cybercrime Directive takes a tougher stance against attacks on information systems, Herbert Smith Freehills LLP, 2013 <http://www.lexology.com/library/detail.aspx?g=d3863b21-3c3b-419e-8a8f-2b007acb3a10> accessed 1 July 2014

[176] Parliament UK, Serious Crime Bill [HL] 2014-15 <http://services.parliament.uk/bills/2014-15/seriouscrime.html> accessed 1 July 2014

[177] Serious Crime Bill, Explanatory Notes, 2014, 1-85, 2 <http://www.publications.parliament.uk/pa/bills/lbill/2014-2015/0001/en/15001en.pdf> accessed 20th January 2015; Serious Crime Act, Explanatory Notes, 2015, 1-85, para.126 < http://www.legislation.gov.uk/ukpga/2015/9/notes/division/3/2> accessed 23rd August 2015

[178] Ibid,29

[179] Serious Crime Act, Explanatory Notes, 2015, 1-85, para.126 < http://www.legislation.gov.uk/ukpga/2015/9/notes/division/3/2> accessed 23rd August 2015

who has responsibility has not consented that the person does the act.[180] *"Material kind"* means causing damage to national security, the economy, the environment or human welfare.[181]

Additionally, the territorial scope for computer misuse offences has been extended, so that extra-territorial jurisdiction applies to the new s.3ZA offence, so that, for example, a UK national, who resides in France, can be prosecuted in the UK or a French national, who resides in the UK and who hacks a computer in France.[182] The amendments provide further clarification, for instance, in respect of s.10 of the Computer Misuse Act 1990.[183] The amendments to the Computer Misuse Act 1990 ensure that the UK fully complies with Directive 2013/40/EU on attacks against information systems.[184]

Apart from the Computer Misuse Act 1990, other legislation can be used to prosecute cyber criminals. For instance, the Obscene Publications Act 1959 and 1964 deals with electronic pornographic offences; the Protection of Children Act 1978 and the Criminal Justice Act 1988 can be evoked in respect of electronic child pornography; the Sexual Offences Act 2003 deals with online and offline sexual grooming; the Public Order Act 1986 and Crime and Disorder Act 1998 render it illegal to incite religious and racial hatred; the Malicious Communications Act 1998 and the Telecommunications Act 1984 contain provisions rendering it a criminal offence to engage in online harassment; the

[180] S.17(8) of the Computer Misuse Act 1990; Serious Crime Act, Explanatory Notes, 2015, 1-85, para.126 < http://www.legislation.gov.uk/ukpga/2015/9/notes/division/3/2> accessed 23rd August 2015
[181] S.3ZA(2) of the Computer Misuse Act 1990; Serious Crime Act, Explanatory Notes, 2015, 1-85, para.126 < http://www.legislation.gov.uk/ukpga/2015/9/notes/division/3/2> accessed 23rd August 2015
[182] Ibid, 31-32
[183] Ibid, 32
[184] Ibid, 29

Copyright, Designs and Patents Act 1998 spells out copyright crimes; and the Terrorism Act 2006 can be used to prosecute various crimes, which are being perpetrated online.[185] For instance, in *R. v Fellows and Arnold,*[186] it was held that the Protection of Children Act 1978 applied when indecent photographs of children were stored in digital format, so that they could be accessed by others and that this constituted active participation in the crime of showing or distributing such images.[187] Yet in *Atkins v DPP*,[188] the prosecution failed since it could not be established that the accused knew that the photos were cached. Jarvie (2003) argues that the imposition of such a requirement burdens the authorities, who have to detect and prosecute paedophiles.[189]

Agate and Ledward (2013) further explicate that s.16 of the Offences Against Person Act 1861 can be invoked when someone threatens to kill another; s.4 of the Protection from Harassment Act 1997 can be used when people are made to fear violence; and s.1 of the Malicious Communications Act 1988 can be invoked when threatening messages are being sent; and s.127 of the Communications Act 2003 can be used when a menacing message is sent[190] and this ensures that threats, including online threats sent via social media, can be combated.[191] For instance, an offence may be made out under s.127 of the Communications Act 2003 when a public order violation is committed by

[185] J. X. Kelly, Computer Misuse Overview, JISC Legal Information, 2007 <http://www.jisclegal.ac.uk/LegalAreas/ComputerMisuse/ComputerMisuseOverview.aspx> accessed 17 June 2014
[186] [1997] 2 All ER 484
[187] N. Jarvie, Control of cybercrime - is an end to our privacy on the Internet a price worth paying? Part 1, 9(3) *Computer and Telecommunications Law Review* 2003, 76-81, 80
[188] [2000] 2 All ER 425
[189] N. Jarvie, Control of cybercrime - is an end to our privacy on the Internet a price worth paying? Part 1, 9(3) *Computer and Telecommunications Law Review* 2003, 76-81, 80
[190] Also see *Chambers v Director of Public Prosecutions* [2012] EWHC 2157 (Admin); [2013] 1 WLR 1833
[191] J. Agate, J. Ledward, Social media: how the net is closing in on cyber bullies, 24(8) *Entertainment Law Review* 2013, 263-268

tweets and the Director of Public Prosecution (DPP) has issued guidelines in 2013 which state that *"those communications that should be robustly prosecuted [are]... those that amount to a credible threat of violence, a targeted campaign of harassment against an individual or which breach court orders, and those communications which may be considered grossly offensive, to which the high threshold must apply."*[192]

Jarvie (2003) remarks that computer fraud can also be prosecuted by placing reliance on the Theft Acts 1968 and 1978, the Forgery and Counterfeiting Act 1981 and the Finance Act 1972.[193] The UK has thus a wide arsenal of statutes to outlaw different forms of cybercrime. Some of the developments within UK cybercrime law have also been driven by virtue of EU law.

1.8 The European Approach Towards Cybercrime

Rychlicki (2006) informs that the EU can fight computer crime by virtue of Title VI of the Treaty of the European Union entitled *"Provisions on police and judicial cooperation in criminal matters."*[194] The 2000 Communication from the Commission[195] firstly affirmed the importance of adopting definitions for high-tech crimes and

[192]Crown Prosecution Service, DPP publishes final guidelines for prosecutions involving social media communications, 20 June 2013 <http://www.cps.gov.uk/news/latest_news/dpp_publishes_final_guidelines_for_prosecutions_involving_social_media_communications/> accessed 20th January 2015; cited from Z. Akhtar, Malicious communications, media platforms and legal sanctions, 20(6) *Computer and Telecommunications Law Review* 2014, 179-187, 182

[193] N. Jarvie, Control of cybercrime - is an end to our privacy on the Internet a price worth paying? Part 1, 9(3) *Computer and Telecommunications Law Review* 2003, 76-81, 78

[194] T. Rychlicki, Legal issues of criminal acts committed via botnets, 12(5) *Computer and Telecommunications Law Review* 2006, 161-167, 164-165; also see M. Jimeno Bulnes, European Judicial Cooperation in Criminal Matters, 5 *European Law Journal* 2003, 614-630

[195] Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions: Creating a safer information society by improving the security of information infrastructures and combating computer-related crime. COM (2000) 890 final. (Brussels, 2000)

sanctions.[196] Also, in 2000, the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union[197] was adopted by the Council pursuant to Article 34 of the Treaty on European Union in order to facilitate law enforcement assistance and co-operation between the Member States.[198] Subsequently, in 2001, the Council Recommendation on contact points maintaining a 24-hour service for combating high-tech crime was adopted.[199] In 2002, Eurojust was established to combat serious crime and its remit overlaps with that of Europol and includes computer fraud and cybercrime.[200] In 2004, the European Network and Information Security Agency (ENISA) was established to safeguard information systems by virtue of the Regulation 460/2004 of the European Parliament and of the Council.[201]

In 2005, the European Union then adopted Council Framework Decision 2005/222/JHA on attacks against information systems.[202] The Council Framework Decision provided that the following acts are rendered criminal offences: illegal data interference, illegal system interference, illegally accessing information systems, and that the Member States had to transpose the regulation by 16 March 2007.[203] However, as the challenges which cybercrime pose have increased, it was necessary to adopt a more comprehensive

[196] T. Rychlicki, Legal issues of criminal acts committed via botnets, 12(5) *Computer and Telecommunications Law Review* 2006, 161-167, 165
[197] [2005] O.J. C197
[198] T. Rychlicki, Legal issues of criminal acts committed via botnets, 12(5) *Computer and Telecommunications Law Review* 2006, 161-167, 165
[199] [2001] O.J. C187; ibid (Rychlicki) 165
[200] Council Decision of February 28, 2002 [2002] O.J. L63; T. Rychlicki, Legal issues of criminal acts committed via botnets, 12(5) *Computer and Telecommunications Law Review* 2006, 161-167, 165
[201] Regulation 460/2004 of the European Parliament and of the Council establishing the European Network and Information Security Agency [2004] O.J. L077/1-11
[202] H. Graux, New Directive on Attacks on Information Systems, Time.lex, 2013 <http://www.timelex.eu/en/blog/detail/new-directive-on-attacks-against-information-systems> accessed 1 July 2014
[203] . Rychlicki, Legal issues of criminal acts committed via botnets, 12(5) *Computer and Telecommunications Law Review* 2006, 161-167, 165

framework.[204] Hence, the Decision has been replaced by Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems (the Cybercrime Directive).[205] Whilst the Framework Decision already set out various definitions for cybercrime, rules for cooperation, jurisdiction and liability, Graux (2013) informs that *"[t]he new Directive further streamlines and enhances the European rules in the fight against cybercrime. While some of the new provisions will clearly be a challenge to implement and apply correctly, they provide a common path to more effective crime fighting."*[206] Graux (2013) also points out that whilst the Directive is similar to its predecessor, it makes clear that certain situations constitute aggravating factors, for instances, *"crimes committed by misusing the personal data of another person, with the aim of gaining the trust of a third party, thereby causing prejudice to the rightful identity owner"* and *"crimes where a significant number of information systems have been affected through the use of a tolls"*, for instance, botnet attacks.[207] Klimek (2015) further explicates that the following four common definitions have been adopted in respect of crimes involving attacks against information systems: illegal interception, illegal system interference, illegal data interference and illegal access to information systems.[208] Resultantly, Member States have to render it a criminal offence when data is illegally intercepted intentionally

[204] H. Graux, New Directive on Attacks on Information Systems, Time.lex, 2013 <http://www.timelex.eu/en/blog/detail/new-directive-on-attacks-against-information-systems> accessed 1 July 2014
[205] Eurocrim-database, Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA, 2013 <http://db.eurocrim.org/db/en/vorgang/252/> accessed 1 July 2014
[206] H. Graux, New Directive on Attacks on Information Systems, Time.lex, 2013 <http://www.timelex.eu/en/blog/detail/new-directive-on-attacks-against-information-systems> accessed 1 July 2014
[207] Ibid
[208] L. Klimek, *European Arrest Warrant* (London, Springer 2015) 112-123

without authorisation and this is done through technology which captures non-publicly transmitted data, including data which is sent through electromagnetic emissions, and this is not a minor case.[209] Yet it has not been defined what a 'not minor' case is. Instead this is left for the Member States to decide in accordance with their domestic laws.[210] For example, the Directive explains that a minor case is one where criminal liability is not imposed.[211]

Furthermore, Member States have to render it a criminal offence when a system is illegally interfered with intentionally and without the person being able to invoke a right to do so and the person does this by gravely interrupting, or hindering its operation by sending, deleting, changing, damaging, transmitting, suppressing or deteriorating information or by preventing access to a system.[212] Member States have to also impose criminal sanctions when data is illegally interfered with intentionally and without the person having a right and this is done by destroying, damaging, altering, deteriorating, or suppressing data or by rendering it inaccessible and this is not a small case.[213] Moreover, Member States have to render it a criminal offence when illegal access is gained to information systems and this is done intentionally and without the person being entitled to have access and this is not a minor case.[214] The Directive also requires Member States to answer information requests within eight hours and additionally Member States are obligated to gather statistical information and report about

[209] Article 6 of the Directive 2013/40/EU on attacks against information systems
[210] Para.11 of the preamble of the Directive 2013/40/EU on attacks against information systems
[211] Ibid
[212] Article 4 of the Directive 2013/40/EU on attacks against information systems
[213] Article 5 of the Directive 2013/40/EU on attacks against information systems
[214] Article 3 of the Directive 2013/40/EU on attacks against information systems

cybercrime incidents and convictions.[215] In this context, Savin and Trzaskowski (2014) further explain that information sharing about cybercrime has also been strengthened through the creation of the European Cybercrime Centre (EC3) by the Commission and which is situated within Europol.[216]

The deadline for transposition was the 4th September 2015.[217] The UK has chosen to opt in[218] and on the 4th June 2014, the Serious Crime Bill (which has now become the Serious Crime Act 2015) was introduced to transpose Directive 2013/40/EU, as well as to combat serious crime and to amend the Computer Misuse Act 1990, as discussed above.[219] Klimek (2015) opines that as a result, criminal law has been harmonised within the EU since rules have been spelled out to define criminal offences, as well as sanctions for attacks on information systems and that mutual co-operation between competent agencies has been strengthened.[220]

In February 2013, an EU cyber security strategy was proposed by the European Commission and as part of this, a Directive on measures to ensure a high common level of network and information security across the Union was proposed (the NIS Directive).[221] During the NATO Advanced Research Workshop on Best Practices for Computer Network Defence: Incident Detection and Response, it was observed that the

---

[215] L. Klimek, *European Arrest Warrant* (London, Springer 2015) 112-123

[216] A. Savin, J. Trzaskowski, *Research Handbook on EU Internet Law* (Cheltenham, Edward Elgar Publishing Limited 2014) 17

[217] ENISA, The Directive on attacks against information systems, A Good Practice Collection for the implementation and application of this Directive 2013, 1-23, 5 <http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/Octopus2013/Presentations/Workshop1/Jo_De_Muynck-ENISA-Octopus.pdf> accessed 1 July 2014

[218] House of Lords, European Union Committee, 5th Report of Session 2013-14, *Follow-up report on EU police and criminal justice measures: The UK's 2014 opt-out decision* (London, TSO 2013) 24

[219] Ashfords, Cybercrime, 2014 <http://www.ashfords.co.uk/cybercrime/> accessed 1 July 2014

[220] L. Klimek, *European Arrest Warrant* (London, Springer 2015) 112

[221] Case Comment, Europe and US divide once again over cyber security, 13(4) *Privacy & Data Protection* 2013, 1, 17, 1; B. Treacy, Expert comment, 13(4) *Privacy & Data Protection* 2013, 2, 2

EU's strategy is based on the following five strategic pillars: firstly, the realisation of cyber resilience; secondly, a significant reduction of cybercrime; thirdly, the development of cybercrime capabilities as part of the Common Security and Defence Policy; fourthly, the development of technical and industrial capital to achieve cyber security; and fifthly, the adoption of a consistent international policy for cyberspace which fosters important EU values.[222] Nagyfejeo (2015) points out that this NIS Directive was adopted by the European Parliament in March 2014.[223]

Savin and Trzaskowski (2014) corroborate that the various EU initiatives are designed to prepare states to deal with cyber attacks, especially the Directive. Member States are required to create a *"National Information Security strategy"* and nominate a domestic agency which is competent and has sufficient human and financial resources to combat and deal with incidents and risks.[224]

The explanatory memorandum of the Directive states that:

> *"the aim of this Directive is to ensure a high common level of network and information security (NIS). This means improving the security of the Internet and the private networks and information systems underpinning the functioning of our societies and economies. This will be achieved by*

[222] IOS Press, *Best Practices in Computer Network Defense: Incident Detection and Response* (Geneva, IOS Press 2014) 71

[223] E. Nagyfejeo, 'Transatlantic collaboration in countering cyberterrorism' in (eds) L. Jarvis, S. Macdonald, T. M. Chen, *Terrorism Online: Politics, Law and Technology* (Abingdon, Routledge 2015) 161

[224] Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union, 7 February 2013, COM(2013) 48 final; A. Savin, J. Trzaskowski, *Research Handbook on EU Internet Law* (Cheltenham, Edward Elgar Publishing Limited 2014) 17

requiring the Member States to increase their preparedness and improve their cooperation with each other, and by requiring operators of critical infrastructures, such as energy, transport, and key providers of information society services (e-commerce platforms, social networks, etc.), as well as public administrations to adopt appropriate steps to manage security risks and report serious incidents to the national competent authorities."[225]

Hence, this Directive ensures that information and network security becomes harmonised within the EU by requiring all market operators, which utilise NIS to adopt organisational and technical steps in respect of cyber risks; and organisations which come within the scope of the Directive have to report security breaches, be subjected to mandatory regulatory audits and have sanctions imposed for failing to comply with the Directive.[226] Hence, just like telecom operators are already required to report security breaches, online service providers, for instance, social networks, large cloud providers, search engines and e-commerce platforms and other providers of traditional infrastructure have to report cyber security breaches.[227] However, no particular security standards are being imposed, but instead stakeholders are requested to work together with the ENISA to promulgate guidelines.[228] Tsagourias and Buchan (2015) state that the objective is to create *"a cooperative network mechanism for information exchange"* by imposing legal obligations on important information society service providers and

[225] Cited from N. Tsagourias, R. Buchan, *Research Handbook on International Law and Cyberspace* (Cheltenham, Edward Elgar Publishing Limited 2015) 415
[226] Case Comment, Europe and US divide once again over cyber security, 13(4) *Privacy & Data Protection* 2013, 1, 17, 1
[227] B. Treacy, Expert comment, 13(4) *Privacy & Data Protection* 2013, 2
[228] Ibid

public agencies, so that adequate steps are taken to deal with security risks and to report grave incidents.[229] A partner at Field Fisher Waterhouse, Stewart Room (2013), observes that *"the scope and magnitude of this new Directive is huge. Obviously, the regulation of cyber risks in utilities, transport, financial services and public authorities is massive in its own right, but it's the wider concept of 'market operator' that really needs to be looked at."*[230]

A proactive approach has thus been adopted to ensure that cybercrime is being strategically combated at the European level and whilst no regional steps have been taken by the Gulf Cooperation Council (GCC) countries, the UAE has also been proactive in the fight against cybercrime.

1.9 Cybercrime Laws in the UAE

Cassim (2009) explains that the UAE was the first GCC country to adopt far-reaching cybercrime legislation in 2006.[231] Beretta (2013) observes that prior to the adoption of Law No.2 of 2006 many of the offences were contained in Law No.15 of 1980 on printed matter and publications, which were then specifically revised for the digital realm.[232] Federal Law No.2 of 2006 on the Prevention of Information Technology

[229] N. Tsagourias, R. Buchan, *Research Handbook on International Law and Cyberspace* (Cheltenham, Edward Elgar Publishing Limited 2015) 416
[230] Cited from Case Comment, Europe and US divide once again over cyber security, 13(4) *Privacy & Data Protection* 2013, 1, 17, 17
[231] F. Cassim, Formulating Specialised Legislation to Address the Growing Spectre of Cybercrime: A Comparative Study, 12(4) *PER* 2009, 1-360, 53
[232] J. Beretta, Privacy in the Middle East: new Cybercrime Law, Privacy and Data Security Law, Coverage and commentary on developments in data protection, Dentons, 2013 <http://www.privacyanddatasecuritylaw.com/category/regulators/page/3> accessed 29 June 2014

Crimes[233] imposes stiff penalties for a broad range of activities, such as gaining access to a website or information system by breaking through a security measure (s.2); procuring the modification or destruction of medical records (s.7); intentionally and unlawfully eavesdropping or intercepting communication (s.8); or using the internet or an information technology device to threaten or blackmail another (s.9). However, Baggili (2011) observes that the sanction system in the UAE is lighter than the one adopted by the UK.[234] Furthermore, Federal Law No.2 of 2006 is not as aligned with the Council of Europe Convention on Cybercrime, and the UAE only created a new department at the Federal Courts in 2009 in order to draft laws for cybercrime.[235]

In 2012, the UAE adopted two more cybercrime laws: Federal Legal Decree No. 5 for 2012 on combating cybercrimes[236] and Law No. 3 of 2012 on establishing the National Electronic Security Authority. These laws were adopted to proactively combat the continuously evolving new cybercrime threats.[237]Federal Legal Decree No. 5 for 2012 on combating cybercrimes makes amendments to the 2006 Federal Legal Decree. Khasawneh and Ahern (2012) describe this as *"a tough new cybercrimes law."*[238] For example, Article 21 proscribes that technology is used to infringe the privacy of others, for instance, by disclosing photographs or conversations or statements, even if they are

[233] aeCert, The Federal Law No. (2) of 2006 on the Prevention of Information Technology Crimes <http://www.aecert.ae/preventionoftechcrimes.php> accessed 29 June 2014
[234] I. Baggili, *Digital Forensics and Cybercrime: Second International ICST Conference, ICDF2C 2010, Abu Dhabi, United Arab Emirates, October 2010, Revised Selected Papers* (London, Springer 2011) 9
[235] Ibid
[236] Ejustice, 2012 <http://ejustice.gov.ae/downloads/latest_laws/cybercrimes_5_2012_en.pdf> accessed 29 June 2014
[237] Also see J. Westby, *International Guide to Combating Cybercrime* (Chicago, American Bar Association Publishing 2003) 14
[238] N. A. Khasawneh, G. Ahern, Cybercrimes law - United Arab Emirates, Eversheds LLP, 5 December 2012 <http://www.lexology.com/library/detail.aspx?g=62f0c34f-0d12-4bbe-bb93-decfc71d4105> accessed 20th January 2015

accurate.[239] The 2012 Federal Legal Decree thus enhances privacy for information which is being made available online and this includes bank account numbers, data information and other details which are being furnished for online payment transactions.[240] Protection of the privacy of individuals is essential especially as there are no data protection laws on a par with the laws in Europe. There is no federal regulator to oversee that data protection is safeguarded, even though citizens have a right to privacy, as defined in Article 31 of the constitution which states that they have a right of *"freedom of corresponding through the post, telegraph or other means of communication and the secrecy thereof shall be guaranteed in accordance with the law"*, but this right does not extend to non-Emiratis, who make up the great majority of residents in the UAE.[241]

However, publishing personal data about a person's family or private life constitutes a criminal offence under Article 378 of Federal Law 3 of 1987 (the Penal Code).[242] Federal Law by Decree No. (3) of 2003 Regarding the Organisation of Telecommunications Sector regulates telecommunication providers and such licensees have to adhere to the Privacy of Consumer Information Policy 2005, which requires that consumer data, including SMS, data and voice transmissions, call patterns and other information are kept private.[243] Some specific legislation applies solely to the economic

[239] Ibid
[240] S. McBride, HH Sheikh Khalifa issues decree on cybercrime, ITP.net, 13 November 2012 <http://www.itp.net/591227-hh-sheikh-khalifa-issues-decree-on-cyber-crime> accessed 23rd January 2015
[241] Practical Law, Data protection in United Arab Emirates: overview, 1 April 2014 <http://uk.practicallaw.com/0-518-8836#> accessed 20th January 2015
[242] Ibid
[243] Practical Law, Data protection in United Arab Emirates: overview, 1 April 2014 <http://uk.practicallaw.com/0-518-8836#> accessed 20th January 2015

free zones, namely the Dubai International Financial Centre Data Protection Law No.1 of 2007, which is quite similar to the European Data Protection Directive and the Dubai Healthcare City Regulation No.7 of 2008, which affirms data protection for health information.[244] However, O'Connell opines that *"these privacy related provisions have not been drafted with the information age in mind."*[245]

Hence, Articles 2 and 21 of the Federal Legal Decree No. 5 for 2012 on combating cybercrimes are key steps - albeit rudimentary – to implement data protection. The former Article rendered it illegal to access electronic networks or information systems or websites without authority, whilst the latter Article proscribes that the privacy of individuals is being evaded through IT, computer networks or electronic information systems without the person consenting to this and without legal authorisation. Moreover, pursuant to Article 39 of the Federal Legal Decree No. 5 for 2012 on combating cybercrimes, operators and owners of computer networks and webpages may face criminal liability if information is published on their network or webpage, or through other technological devices, when illegal content is published, or they fail to take illegal content down upon being notified. Federal Law No.15 of 1980 Governing Publications and Publishing delineates what types of publications are proscribed.[246]

---

[244] Norton Rose, Key data privacy and intellectual property issues in the UAE, November 2011 <http://www.nortonrosefulbright.com/knowledge/publications/54334/key-data-privacy-and-intellectual-property-issues-in-the-uae> accessed 20th January 2015

[245] N. O'Connell, Data Protection and Privacy Issues in the Middle East, Tamimi, 12/13 December 2011 <http://www.tamimi.com/en/magazine/law-update/section-6/january-february-1/data-protection-and-privacy-issues-in-the-middle-east.html> accessed 20th January 2015

[246] N. A. Khasawneh, G. Ahern, Cybercrimes law - United Arab Emirates, Eversheds LLP, 5 December 2012 <http://www.lexology.com/library/detail.aspx?g=62f0c34f-0d12-4bbe-bb93-decfc71d4105> accessed 20th January 2015

Under Federal Legal Decree No. 5 for 2012 on combating cybercrimes, all types of cybercrime are being criminalised and custodial sentences and/or fines can be imposed and enforcement agencies have been granted extra-territorial enforcement powers. Al Tamimi (2013) corroborates that the themes of the 2012 law can be grouped into the following categories: "*IT security, state security and political stability, morality and proper conduct, financial and commercial issues and miscellaneous"* matters.[247] However, Human Rights Watch (2012) observes that the Federal Decree No.5 for 2012 is an affront to free speech and results in it being very difficult for normal citizens or activists to voice their concerns.[248] This is because the provisions are very wide and ambiguous, so that individuals can be easily prosecuted for criticising officials. Yet Human Rights Watch (2012) concedes that not all provisions are directed at curtailing free speech, but that provisions also ensure that, for instance, sectarian or racist views are not published online.[249] For instance, Iaccino (2015) informs about a 2015 Federal Supreme Court (FSC) unreported decision in which a person violated the law by swearing at a colleague in a WhatsApp message and was as a result fined $68,000 (the equivalent of £42,769) and deported.[250]

Law No. 3 of 2012 on Establishing the National Electronic Security Authority creates the National Electronic Security Authority (NESA), which is responsible for

[247] Al Tamimi & Company, Developments in the UAE Cybercrimes Law, The Lawyer 2013 <http://www.thelawyer.com/briefings/developments-in-the-uae-cyber-crimes-law/3004681.article> accessed 20 June 2014
[248] Human Rights Watch, UAE: Cybercrimes Decree Attacks Free Speech, Threatens Peaceful Activists, Ordinary Citizens Alike, 2012 <http://www.hrw.org/news/2012/11/28/uae-cybercrimes-decree-attacks-free-speech> accessed 29 June 2014
[249] Ibid
[250] L. Iaccino, UAE cybercrime: Man faces £42,000 fine for swearing at colleague over WhatsApp, International Business Times, 18 June 2015 <http://www.ibtimes.co.uk/uae-cybercrime-man-faces-42000-fine-swearing-colleague-over-whatsapp-1506803> accessed 22nd August 2015

"organis[ing] protection for the Communication Network and Information Systems in the State and [for] develop[ing], amend[ing] and us[ing] the necessary methods in [the] Electronic Security domain" and which co-operates with aeCERT and the Telecommunications Authority.[251] On the 25th June 2014, the NESA informed that it will publish various strategies, standards and policies, so that the efforts to combat cyber security become strategically aligned at the national level.[252] Subsequently, NESA (2015) published its Critical Information Infrastructure Protection Policy and Information Assurance Standards which endorse a threat based approach and make use of recognised security guidance and standards, for instance ISO 27001.[253] Downton points out that NESA lists 24 different threats in accordance with the percentage in which they have been reported to have occurred.[254] A range of controls which have been adopted by others are listed next to the various threats, as well as other sub-controls.[255] Downton (2015) explains that whilst this appears as a good starting point, this may not be sufficient since advanced threats will not be mitigated against by standardised security approaches.[256]

[251] J. Beretta, Privacy in the Middle East: new Cybercrime Law, Privacy and Data Security Law, Coverage and commentary on developments in data protection, Dentons, 2013 <http://www.privacyanddatasecuritylaw.com/category/regulators/page/3> accessed 29 June 2014
[252] ITP.net, UAE cyber-security authority unveils policies, standards, 2014 <http://www.itp.net/598777-uae-cyber-security-authority-unveils-policies-standards> accessed 29 June 2014
[253] B. Downton, NESA – The New Standard of Information Security in the UAE, MWR InfoSecurity, 6 April 2015 <https://www.mwrinfosecurity.com/articles/nesa-the-new-standard-of-information-security-in-the-uae/> accessed 20th August 2015
[254] Ibid
[255] Ibid
[256] Ibid

In September 2014, it was announced that a cyber command will be created within the UAE military and which will work in parallel to the NESA.[257] A cybercrime unit has also been created within Abu Dhabi's State Security Apparatus and a Department of Anti-Electronic Crimes has been formed as part of Dubai police.[258]Yet the adoption of cybercrime offences and the creation of a specialised agency entrusted with cyber security and other units/departments to combat cybercrime are insufficient to deal with the emerging threat which emanates from cybercrime. For instance, Dr Saud Al Junaibi (2014) highlighted at the Abu Dhabi Electronic Warfare GCC conference in 2014 that most cyber criminals try to attack critical infrastructure and critical services and that *"[d]ata detection systems like Scada (Supervisory Control and Data Acquisition) are still behind in terms of protection from cyber threats"* since these systems are only programmed to provide services and are therefore only receptive to gathering data from different sources and when attackers access such systems, important services can be disrupted.[259] He further pointed out that network security of these systems is not coordinated and it is therefore important to organise a *"Technical Standards Forum"*, but also acknowledged that NESA is facilitating that government agencies and industry are adopting international standards to cope with *"cyber electronic warfare."*[260] In this context, His Excellency Jassem Bu Ataba Al Zaabi (2014), General Director, noted that *"[c]ybersecurity is one of the biggest economic and national security challenges*

[257] B. Thomas, UAE Military To Set Up Cyber Command, Defenseworld.net, 30 September 2014 <http://www.defenseworld.net/news/11185/UAE_Military_To_Set_Up_Cyber_Command#.VMVEmyws q6Q> accessed 20th January 2015
[258] Reporters Without Borders, United Arab Emirates: Tracking "cyber-criminals", 2014 <http://12mars.rsf.org/2014-en/2014/03/11/united-arab-emirates-tracking-cyber-criminals/> accessed 20th January 2015
[259] C. Malek, UAE needs better protection of critical infrastructure, The National, 19 November 2014 <http://www.thenational.ae/uae/technology/uae-needs-better-protection-of-critical-infrastructure> accessed 22nd August 2015
[260] Ibid

countries face in the twenty-first century. The National Electronic Security Authority was established in line with this modern reality and as soon as the Authority was in place, we immediately initiated a thorough review of federal efforts to defend and protect the nation's ICT infrastructure. This announcement falls in line with the process we are currently engaged in which puts all necessary policies and standards in place to ensure a comprehensive approach to securing the nation's digital infrastructure".[261]

The researcher argues that police officers can only effectively secure the digital realm if it is made more transparent. This in turn requires that data is retained and surveillance takes place, as occurs for instance, in the UK, but this has to be administered in a way which both protects data and respects the right to privacy.

[261] B. Thomas, UAE Military To Set Up Cyber Command, Defenseworld.net, 30 September 2014 <http://www.defenseworld.net/news/11185/UAE_Military_To_Set_Up_Cyber_Command#.VMVEmywsq6Q> accessed 20th January 2015

1.10 The UK Approach Towards Data Protection

1.10.1 The Right to Privacy

Privacy means *"freedom from unauthorized intrusion."*[262] Gillespie (2009) emphasises that the notion of private information is crucial in respect of surveillance.[263] However, the director of Liberty, James Welch (2014) summarises the problem as follows: *"The security services consider that they're entitled to read, listen to and analyse all our communications on Facebook, Google and other US-based platforms. If there was any remaining doubt that our snooping laws need a radical overhaul, there can be no longer. The agencies now operate in a legal and ethical vacuum; why the deafening silence from our elected representatives?"*[264]

In the UK, the right to privacy traditionally did not exist, but Fenwick explains that instead equity or tort claims could be brought, for instance, for trespass, copyright, defamation and breach of confidence; accordingly, the right could be indirectly enforced.[265] For instance, in 1997, before the enactment of the Human Rights Act 1998, Lord Irvine opined *"that the true view is that the courts will be able to adapt and develop the common law by relying on existing domestic principles in the laws of*

---

[262] Merriam Dictionary <http://www.merriam-webster.com/dictionary/privacy> accessed 20th January 2015; H. Sarfaraz, Surveillance, privacy and cyber law, 20(7) Computer and Telecommunications Law Review 2014, 189-194, 189

[263] A. A. Gillespie, Regulation of internet surveillance, 4 *European Human Rights Law Review* 2009, 552-565, 554

[264] Cited from Z. Akhtar, Malicious communications, media platforms and legal sanctions, 20(6) *Computer and Telecommunications Law Review* 2014, 179-187, 184

[265] H. Fenwick, *Civil Liberties and Human Rights* (4th edn, Abingdon, Routledge-Cavendish 2007) 807

trespass, nuisance, copyright, confidence and the like, to fashion a common law right to privacy."[266]

Richardson et al (2012) opine that the breach of confidence played a particularly important role to distinguish private from public information.[267] Von Bar (2009) notes that the traditional test to identify whether there was a breach of confidence was famously espoused by Megarry J in *Coco v AN Clark (Engineers) Ltd,*[268] in which he stated "[f]irst, the information itself … must have the necessary quality of confidence about it.[269] Secondly, that information must have been imparted in circumstances importing an obligation of confidence. Thirdly, there must be an unauthorised use of that information to the detriment of the party communicating it."[270] This claim therefore became the main tool to enforce privacy.[271] *Coco v AN Clark (Engineers) Ltd* despite being a High Court case and therefore, technically, only binding to lowers courts, it managed to recast the doctrine of confidence in a way that responded to a change in the broader social background.[272] The case became a starting point in many subsequent cases, despite only being a High Court decision[273] and had led to major academic debates about the breadth of equitable confidence; Gareth Jones argues that:

'[e]*quity, to borrow a metaphor, should not be past the age of child-bearing. A defendant who has taken good care not to enter any relationship of any sort with the plaintiff and who has obtained confidential information by reprehensible means should be in no better position than a defendant who is given and deliberately breaches the plaintiff's confidence'*[274].

While Jones' co-writer Robert Goff recast the elements of confidence in such a way as to encompass unauthorised (but not necessarily nefarious) takings of information, even

---

[266] House of Lords Debate, 24 November 1997, col 785; J. Cooper, A. Marshall-Williams, *Legislating for Human Rights, The Parliamentary Debates on the Human Rights Bill* (Portland, Hart Publishing 2000) 222

[267] M. Richardson, M. Bryan, M. Vranken, K. Barnett, *Breach of Confidence, Social Origins and Modern Developments* (Cheltenham, Edward Elgar Publishing Ltd 2012) 1

[268] (1969) RPC 41

[269] C. Von Bar, *Non-Contractual Liability Arising out of Damage Cause to Another* (Munich, European Law Publishers 2009) 54

[270] *Coco v AN Clark (Engineers) Ltd* (1969) RPC 41, per Megarry J at 7

[271] Younger Committee, Report on Privacy, 1972, p. 26; also see *Duchess of Argyll v Duke of Argyll* [1967] Ch 302; *AG v Guardian Newspapers (No 2)* [1990] AC 109

[272] T.D.C. Bennet, (2018) 'Judicial activism and the nature of "misuse of private information" Communications Law, 23(2) 74-88.

[273] *Stephens v Avery* [1988] FSR 510.

[274] G. Jones, "Restitution of Benefits Obtained in Breach of Another's Confidence' (1970) 86 LQR 463, 482.

in circumstances where there was no prior relationship of confidence between the parties or express obligation of confidence placed on the confidant.[275]

Smart states that when the Human Rights Act 1998 was enacted the right to privacy became recognised, though Article 8 was already recognised by the UK prior to this.[276] The right to privacy is enshrined in Article 8 of the European Convention on Human Rights (ECHR), it states:

> *"(1) Everyone has the right to respect for his private and family life, his home and his correspondence.*
>
> *(2) There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."*

The effect of s.3 of the Human Rights Act 1998 is that *"[s]o far as it is possible to do so, primary legislation and subordinate legislation must be read and given effect in a way which is compatible with the Convention rights."*[277] S.6 of the Human Rights Act 1998 ensures that the right to privacy has only a vertical effect (i.e. is only enforceable

[275] T.D.C. Bennet, (2018) 'Judicial activism and the nature of "misuse of private information" Communications Law, 23(2) 74-88.
[276] U. Smartt, *Media & Entertainment Law* (2nd edn, Abingdon, Routledge 2014) 93
[277] S.3 of the Human Rights Act 1998

against public authorities, excluding the police), but courts can *"develop the underlying common law in such a way to include the value of" privacy."*[278]

Irrespective of whether or not the right to privacy has only a vertical effect, the European Court of Human Rights has made clear that covert surveillance can breach Article 8(1) of the ECHR and has to be justified under Article 8(2).[279] However, McArthur opines that privacy cannot be expected on the internet since it constitutes a public space, and that privacy may only be possible when tracking software is blocked or one's identity is concealed.[280] Yet such a stance may hamper innovation, as it would imply that trade secrets could not be protected. It also conflicts with Article 8(1). The European Court of Human Rights also does not regard that the simple fact that something takes place in public means that there is no privacy, as illustrated by *Von Hannover v Germany*.[281] Instead, *Von Hannover* makes clear that privacy does not depend on location and that a public versus private division is too simple, but instead *"a test of a reasonable expectation of privacy or, more broadly still, of control of private information is more satisfactory."*[282]

Whilst this case did not deal with online privacy, Gillespie (2009) therefore disagrees with McArthur (2001) and gives the additional example of using an online service,

---

[278] A. Gillespie, *The English Legal System* (Oxford, Oxford University Press 2013) 148; also see *Wainwright v Home Office* [2003] 3 WLR 1137 where it was stated "In this country, unlike the United States of America, there is no over-arching, all-embracing cause of action for 'invasion of privacy" cited from J. Gordley, A. Taylor von Mehren, *An Introduction to the Comparative Study of Private Law, Readings, Cases, Materials* (Cambridge, Cambridge University Press 2006) 283

[279] *Malone v United Kingdom* (1985) 7 EHRR 14 ECtHR; *Halford v United Kingdom* (1997) 24 EHRR 523 ECtHR; A. A. Gillespie, Regulation of internet surveillance, 4 *European Human Rights Law Review* 2009, 552-565, 554

[280] R.L. McArthur, Reasonable Expectations of Privacy, 3 *Ethics and Information Technology* 2001, 123-128, 126

[281] (2005) 40 EHRR 1 ECtHR

[282] H. Fenwick, *Civil Liberties and Human Rights* (4th ed, Abingdon, Routledge 2009) 836

which specifically offers secure back up storage.[283] Coleman (2006) corroborates that the essence of privacy is to prevent access to information, particularly emails.[284] In contrast, McArthur (2001) argues that the fact that access can be restricted does not change the public nature of the internet since electronic measures can be used to circumvent any access restrictions, but Gillespie (2009) perceives that such perception does not fit the jurisprudence of the European Court of Human Rights, especially the reasonable expectation test in *Von Hannover*.[285] Consequently, when surveillance takes place, this has to be authorised in order to ensure that there is compliance with Article 8(2) of the ECHR..

The European Court of Human Rights has also held that this is necessitated by rejecting that administrative authority is sufficient to satisfy the requirement in Article 8(2) to be *"in accordance with the law."*[286] Systematic recording was also found to breach Article 8(1) of the ECRH[287] and the same principle also applies in the online context, as made clear by the European Court of Human Rights in *Copland v United Kingdom*.[288] In this case, the Court stated that *"[a]ccording to the Court's case law, telephone calls ... are covered by the notions of 'private life' and 'correspondence' for the purposes of Art 8(1) ... It follows logically that emails sent from work should be similarly protected*

[283] A. A. Gillespie, Regulation of internet surveillance, 4 *European Human Rights Law Review* 2009, 552-565, 556
[284] S. Coleman, E-mail, terrorism, and the right to privacy, 8 *Ethics and Information Technology* 2006, 17-27, 20
[285] A. A. Gillespie, Regulation of internet surveillance, 4 *European Human Rights Law Review* 2009, 552-565, 556
[286] *Khan v United Kingdom* (2001) 31 EHRR 45 ECtHR; ibid (Gillespie) 556
[287] *Friedl v Austria* (1996) 21 EHRR 83 ECtHR
[288] (2007) 45 EHRR 37 ECtHR

under Art 8, as should information derived from the monitoring of personal internet usage."[289]

In *Amann v Switzerland,*[290] the European Court of Human Rights also stated that *"tapping and other forms of interception of telephone conversations constitute a serious interference with private life and correspondence and must accordingly be based on a 'law' that is particularly precise. It is essential to have clear, detailed rules on the subject, especially as the technology available for use is continually becoming more sophisticated."* In light of the decision, Taylor (2003) points out that surveillance methods have to be regulated by law to ensure that there is compliance with Article 8(1), i.e. that the interference is *"in accordance with law."*[291] Furthermore, Gillespie (2009) argues that an authorisation is required to conduct directed surveillance pursuant to the RIPA.[292]

The *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources*[293] case mentioned above also mandates that fundamental rights cannot be seriously interfered with.[294] The Court of Justice of the European Union (CJEU) observed that data retention allows that the person is identified, the place and time of a communication, how often the person communicates with particular persons and this means that very private information is being made available, for instance, about their everyday habits, their daily activities and home, their social environment, etc. and this

---

[289] *Copland v United Kingdom* (2007) 45 EHRR 37 ECtHR, at 41
[290] App. No.27798/95, Judgment of February 16, 2000
[291] N. Taylor, Policing, privacy and proportionality, *European Human Rights Law Review* 2003, 86-100, 91
[292] A. A. Gillespie, Regulation of internet surveillance, 4 *European Human Rights Law Review* 2009, 552-565, 559
[293] (C-293/12) [2014] 3 W.L.R. 1607 (ECJ (Grand Chamber))
[294] M.-P. Granger, K. Irion, The Court of Justice and the Data Retention Directive in Digital Rights Ireland: telling off the EU legislator and teaching a lesson in privacy and data protection, 39(6) *European Law Review* 2014, 835-850, 846

seriously breaches the private life and violates the persons' personal data, particularly in circumstances where data is retained and used without the knowledge of the person.[295] Yet the Court considered that such data retention was justified in the name of public security, but that the principle of proportionality had been stretched too far by the EU legislature.[296] Indeed, proportionality can be more readily made out when adequate protective safeguards have been adopted, as made clear in *Klass v Germany*[297] where it was said that *"[o]ne of the fundamental principles of a democratic society is the rule of law ... [which] implies, inter alia, that an interference by the executive authorities with an individual's rights should be subject to an effective control..."*[298]

The Council of the European Union also notes that the court will not *"satisfy itself with anything less than a strict assessment of the proportionality and necessity of measures that constitute serious restrictions to fundamental rights, however legitimate the objectives pursued by the EU legislature."*[299] Yet Granger and Irion (2014) point out that the Grand Chamber in *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources*[300] has not defined what amounts to a serious interference and how to conduct such an assessment.[301] Nonetheless, they corroborate that the decision mandates *"a new level of responsibility to protect fundamental rights,"* imposes *"a novel strict judicial scrutiny test"* and invalidates EU law, which breaches

---

[295] Case Comment, Data retention Directive invalid, says ECJ, 319 *EU Focus* 2014, 14-16, 15
[296] Ibid
[297] (1979-80) 2 E.H.R.R. 214, 55
[298] Cited from N. Taylor, Policing, privacy and proportionality, *European Human Rights Law Review* 2003, 86-100, 89
[299]Council of the European Union, General Secretariat, Judgment of the Court of 8 April 2014 in joined Cases C-293/12 and C-594/12, 909/14 JUR, 5 May 2014; cited from M.-P. Granger, K. Irion, The Court of Justice and the Data Retention Directive in Digital Rights Ireland: telling off the EU legislator and teaching a lesson in privacy and data protection, 39(6) *European Law Review* 2014, 835-850, 846
[300] (C-293/12) [2014] 3 W.L.R. 1607 (ECJ (Grand Chamber))
[301] *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources* (C-293/12) [2014] 3 W.L.R. 1607 (ECJ (Grand Chamber), at 37

Charter rights and provides substantive guidance to EU and national law-makers in respect of data protection and privacy rights. Granger and Irion (2014) therefore think that the decision re-emphasises constitutionalism and human rights as crucial building blocks for European integration.[302] Hence, even in a *"Big Data era"* the requisite threshold for data and privacy protection remains high within the EU.[303] This is also in line with the jurisprudence promulgated by the European Court of Human Rights, for instance, in *Rotaru v Romania,*[304] where it was noted that *"[s]tates do not enjoy unlimited discretion to subject individuals to secret surveillance or a system of secret files. The interest of a state in protecting its national security must be balanced against the seriousness of the interference with the applicant's right to respect for his or her private life"* and in *Klass v Germany*,[305] it was observed that *"powers of secret surveillance of citizens are tolerable under the Convention only in so far as strictly necessary for safeguarding democratic institutions."*[306] Accordingly, cyber security is thus not a blanket reason to permit unlimited surveillance and data retention, but this has to be balanced against the right to private life.[307] The concept of confidentiality, as developed by cases which have created the common law claim for breach of confidence, has been strengthened by the human rights claim. Privacy is also protected by virtue of the UK Data Protection Act 1998.

---

[302] M.-P. Granger, K. Irion, The Court of Justice and the Data Retention Directive in Digital Rights Ireland: telling off the EU legislator and teaching a lesson in privacy and data protection, 39(6) *European Law Review* 2014, 835-850, 849
[303]Ibid, 850
[304] (2000) 8 BHRC 449
[305] (1979) 2 EHRR.305
[306] Cited from N. Taylor, Policing, privacy and proportionality, *European Human Rights Law Review* 2003, 86-100, 97
[307] Also see ibid

1.10.2 The UK Data Protection Act 1998 and the European Approach Towards Maintaining Privacy

In a digital world, privacy is particularly important to protect individuals and businesses from cybercrime. McLeod and Hare (2010) explain that the UK Data Protection Act 1998 regulates the manner in which personal data about individuals, who are alive, is being managed and processed.[308] Bainbridge (2004) notes that the Act *"does not affect any right to relief for breach of confidence or defamation, in appropriate cases."*[309]

Smith (2007) explains that the UK approach to data protection is based on Directive 96/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data, which was adopted *"to protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data, and to prevent the restriction or prohibition of the free flow of personal data between Member States for privacy reasons."*[310] Those, who process personal data in the UK, have to inform the Information Commissioner.[311]

Data is defined by s.1 of the Data Protection Act 1998, as information, which is processed with automatically operating equipment after instructions are given to do so, when the data is recorded and there is intention that the processing shall take place with

[308] J. McLeod, C. Hare, *How to Manage Records in the e-Environment* (Abingdon, Routledge, 2010) 65
[309] Cited from D. Bainbridge, *Introduction to Computer Law* (5th edn, Harlow, Pearson Education Ltd 2004) 489; Also see *Michael Douglas v Hello! Ltd (No. 2)* [2003] EWHC 786 (Ch)
[310] Article 1 of Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data; G. J. J. Smith, Bird & Bird, *Internet Law and Regulation* (4th edn, London, Sweet & Maxwell 2007) 687
[311] S.17 of the Data Protection Act 1998

the equipment, the record is made in a relevant filing system[312] and there is such intention and the information does not fall within paragraph (a)-(c) and is a record, which is accessible, which meets the definition in s.68 of the Data Protection 1998. The Act is only invoked when there is personal data and this means data from which it is possible to identify a living individual or their expression of opinion.[313] Accordingly, the Data Protection Act 1998 is only applicable when it is possible to identify an individual and the person is alive. In *Durant v Financial Services Authority,*[314] personal data was narrowly interpreted as data which is *"biographical in a significant sense"* and requiring that *"the information has the putative data subject as its focus."*[315]

The Data Protection Act 1998 requires data controllers to adhere to eight important principles, which range from, processing data lawfully and fairly, not over excessively processing data, and ensuring that personal data is accurate to not transferring personal data to a country outside the European Economic Area when there is insufficient protection in that country.[316]

Gulwirth et al (2009) explain that the Data Protection Act 1998 places much emphasis on data subjects giving consent to their personal data being collected, though personal

[312] A relevant filing system means "…any set of information relating to individuals to the extent that, although the information is not processed by means of equipment operating automatically in response to instructions given for that purpose, the set is structured, either by reference to individuals or by reference to criteria relating to individuals, in such a way that specific information relating to a particular individual is readily accessible" s.1(1) of the Data Protection Act 1998
[313] S.1(1) of the Data Protection Act 1998
[314] [2003] EWCA Civ 1746
[315] *Durant v Financial Services Authority* [2003] EWCA Civ 1746, para.28
[316] Schedule 1 of the Data Protection Act 1998; also see the Information Commissioner's Office; Data protection principles, 2014 <ico.org.uk/for_organisations/data_protection/the_guide/the_principles> accessed 1 July 2014

data can also be processed if any of the conditions in Schedule 2 of the Data Protection Act 1998 are met, for instance, if this is needed to for a contract.[317] Yet they criticise this because as a result the purpose for which data is being collected is being disregarded.[318]

Gooch and Williams (2007) note that data subjects have a right to write to the organisation, which holds information about them and request that they see what data is held.[319] Yet the House of Lords Science and Technology Committee Report on Personal Internet Security 2007 observes that the remedies are inadequate and as a result there is no *"practical incentive for those holding customer data to take steps to protect it."*[320] However, in light of the important *Google Spain SL v Agencia Espanola de Proteccion de Datos (AEPD)*[321] case heard by the CJEU, data protection has been given further importance within the online context. In this case a preliminary reference was brought to determine whether the Data Protection Directive could be evoked against search engines, for instance, Google and even in circumstances where the data processing did not take place in the EU, persons could require that their personal data was removed from the search engine.[322] The CJEU found that the fact that the physical server is not located in Europe does not matter, as Google had a branch in a Member State. As search engines control personal data they were bound by EU data protection law and

[317] S. Gutwirth, Y. Poullet, P. De Hert, *Reinventing Data Protection?* (Springer 2009) 84
[318] Ibid
[319] G. Gooch, M. Williams, *A Dictionary of Law Enforcement* (Oxford, Oxford University Press 2007) 105
[320] House of Lords Science and Technology Committee, Personal Internet Security, Volume I: Report, 5th Report of Session 2006-2007, para.5.34 <http://www.publications.parliament.uk/pa/ld200607/ldselect/ldsctech/165/165i.pdf> accessed 1 July 2014
[321] (C-131/12) (2014) 164(7607) NLJ 20
[322] Z. Akhtar, Malicious communications, media platforms and legal sanctions, 20(6) *Computer and Telecommunications Law Review* 2014, 179-187, 185

individuals are entitled, if they meet certain criteria, to request search engines to remove their personal information. Even information which was accurate may no longer be collected when the information is irrelevant, inadequate or excessive in respect of the aim of the data. What it amounts to is this, individuals are not automatically entitled to be forgotten, but a balance has to be struck with other rights, e.g. freedom of speech.[323] Akhtar (2014) explains that as a result of the decision an assessment has to be made each time to evaluate: the type of information, whether it constitutes sensitive information about a person's private life, what interest the public have in being able to access the information, and the role the person plays in public life.[324]

More recently, on 14 September 2017 a new Data Protection Bill was published in the UK which has been introduced in its Parliament. It aims to overhaul and update the UK data protection laws for an increasingly digital age and economy.[325] It is also in preparation for Britain's departure from the EU (also known as 'Brexit'), ensuring that strong data laws and appropriate safeguards are in place so that Britain can trade across international borders. Key features of the new bill are: implementation and clarification of the GDPR – which will apply from 25 May 2018 - in the UK context, new criminal offences related to data, empowering people to be able to withdraw their consent with respect to their personal data, and enabling them to access and/or restrict the way that

[323] *Google Spain SL v Agencia Espanola de Proteccion de Datos (AEPD)* (C-131/12) (2014) 164(7607) NLJ 20, 56, 80, 93, 85; Z. Akhtar, Malicious communications, media platforms and legal sanctions, 20(6) *Computer and Telecommunications Law Review* 2014, 179-187, 185-186

[324] Ibid (Akhtar) 186

[325] R. Hill, 'UK Data Protection Bill lands: Oh dear, security researchers – where's your exemption?' *The Register*, September 2017 <https://www.theregister.co.uk/2017/09/14/messy_data_protection_bill_lands_in_parliament/> accessed December 2017

organisations use their personal data, and the imposition of fines of up to €20m / £17m for businesses who are found guilty of serious data breaches.[326]

Having such data protection laws encourages businesses to safeguard data and it is therefore important for the UAE to adopt equally strong measures as this can safeguard against cybercrime. Correspondingly, the UAE should adopt specific data protection standards for enforcement agencies, as the European Union has done. De Azevedo Cunha (2013) points out that Declaration 21 on the protection of personal data in the fields of judicial and police cooperation in criminal matters, which is an annex to the Treaty of Lisbon, states *"that specific rules on the protection of personal data and the free movement of such data in the fields of judicial cooperation criminal matters and police cooperation based on Article 16 of the Treaty on the Functioning of the European Union may prove necessary because of the specific nature of these fields."*[327] Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters delineates the necessary data protection measures which have to be adopted when the police and judiciary cooperate in relation to criminal matters.[328] Article 5 of the Framework Decision makes clear that Directive 95/46/EC does not apply when *"processing operations concerning public security, defence, state security or the*

[326] 'Data Protection Bill Overview Factsheet', *Department for Digital, Culture, Media and Sport*, September 2017 <https://www.gov.uk/guidance/data-protection-bill-overview> accessed December 2017

[327] M. V. de Azevedo Cunha, *Market Integration Through Data Protection, An Analysis of the Insurance and Financial Industries in the EU* (London, Springer 2013) 44

[328] Parliament UK, Fifty-ninth Report of Session 2010-12 - European Scrutiny Committee, Data processing in the framework of police and criminal cooperation <http://www.publications.parliament.uk/pa/cm201012/cmselect/cmeuleg/428-liv/42810.htm> accessed 1 July 2014; also see R. Funta, EU-USA Privacy Protection Legislation and the Swift Bank Data Transfer Regulation: A Short Look, 5(1) *Masaryk University Journal of Law and Technology* 2011, 23-33, 26

activities of the State in areas of criminal law" are conducted. Ismaiel and Cieh (2013) explain that whilst the European approach is *"the world's leading and most comprehensive model"*, there is a *"need for change."*[329]

1.10.3 The 2012 European Reform Proposals

The European data protection rules were formulated in 1995 and the digital space has since then tremendously increased. As a result, these rules do not deal with data, which is being *"processed for law enforcement purposes."*[330] On the 12th March 2014, the European Parliament therefore expressed its support for the reform proposal promulgated by the European Commission, particularly against the background of the Snowden revelations about the US "*data spying scandals."*[331]

The EU's Justice Commissioner, Vice-President Viviane Reding (2014) stated *"[d]ata protection in the European Union is a fundamental right. Europe already has the highest level of data protection in the world. With the EU data protection reform which was proposed exactly two years ago – in January 2012 – Europe has the chance to make these rules a global gold standard. These rules will benefit citizens who want to be able to trust online services, and the small and medium sized businesses looking at a single market of more than 500 million consumers as an untapped opportunity. The European*

---

[329] N. Ismail, E. L. Y. Cieh, *Beyond Data Protection, Strategic Case Studies and Practical Guidance* (London, Springer 2013) 3

[330] European Parliament News, Q&A on EU data protection reform, 2014 <http://www.europarl.europa.eu/news/en/news-room/content/20130502BKG07917/html/QA-on-EU-data-protection-reform> accessed 30 June 2014

[331] European Commission Memo, Progress on EU data protection reform now irreversible following European Parliament vote, 2014 <http://europa.eu/rapid/press-release_MEMO-14-186_en.htm> accessed 30 June 2014

Parliament has led the way by voting overwhelmingly in favour of these rules. I wish to see full speed on data protection in 2014."[332]

Reding (2013) explains that the aim of the Network Information Security Directive 2016/1148[333] is to create a *"resilient digital single market"* in order to better cope with cyber-attacks and that the *"EU's Data Protection rules and Cyber Security Strategy [are] two sides of the same coin."*[334] Banck (2013) explains that the European data reform requires digital market operators to notify data breaches to the data protection authority, as well as to a security authority, which has to be established by each Member State under the European Commission Cyber Directive project, as well as to adopt organisational and technical measures to deal with risks, which emanate from information systems and security networks in their control.[335]

Cannataci (2013) further corroborates that Directive 95/46/EC is replaced by General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679)[336], which sets out a framework and the Network Information Security Directive 2016/1148, which replace

[332] Cited from European Commission Memo, Data Protection Day 2014: Full Speed on EU Data Protection Reform, 2014 <http://europa.eu/rapid/press-release_MEMO-14-60_en.htm> accessed 30 June 2014

[333] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union

[334] V. Reding, The EU's Data Protection rules and Cyber Security Strategy: two sides of the same coin, European Commission, 2013 <http://europa.eu/rapid/press-release_SPEECH-13-436_en.htm> accessed 30 June 2014

[335] A. Banck, EU Cyber Directive: How does it relate to Data Protection Law and Data Protection Reform? Privacy Europe, 2013 <http://www.privacy-europe.com/blog/eu-cyber-directive-how-does-it-relate-to-data-protection-law-and-data-protection-reform/> accessed 1 July 2014

[336] European Commission, LIBE Committee vote backs new EU data protection rules, 22 October 2013, MEMO/13/923 <http://europa.eu/rapid/press-release_MEMO-13-923_en.htm> accessed 20th January 2015; European Commission, Data Protection Day 2014: Full Speed on EU Data Protection Reform, 27 January 2014, MEMO/14/60 <http://europa.eu/rapid/press-release_MEMO-14-60_en.htm> accessed 20th January 2015

Framework Decision 2008/977/JHA16 in order to spell out the principles when personal data can be processed to prevent, detect, investigate or prosecute crimes and for interconnected judicial activities.[337] Akhtar explicates that the GDPR modernises the European data protection laws and grants citizens new rights, including having personal information destroyed[338] and the company, as opposed to the individual, has the burden of proof to show that the data should not be deleted.[339] Article 3 of the GDPR also confirms that irrespective of the physical server, when services are provided within Europe, European data protection rules have to be adhered to. Member States are also required to adopt domestic legislation to strike a balance between freedom of expression, which encompasses data processing, so that the media can access it and with data protection.[340]

Also, as discussed above, since 2013, communications service providers have to report breaches within 24 hours to their regulator and inform the data subject about a breach, which is *"likely to adversely affect the personal data or privacy"* of an individual pursuant to Commission Regulation 611/2013 of June 2013 on the measures applicable to the notification of personal data breaches under Directive 2002/58/EC of the European Parliament and of the Council on privacy and electronic communications and under the GDPR, and this obligation is extended to all those, who act as data controllers,

[337] J. A. Cannataci, Defying the logic, forgetting the facts: the new European proposal for data protection in the police sector, 4(2) *European Journal of Law and Technology* 2013 <http://ejlt.org/article/view/284/390> accessed 1 July 2014; also see C. Walker, EU rules on breach notification, Olswang, 2014 <http://www.olswang.com/articles/2014/06/eu-rules-on-breach-notification/> accessed 1 July 2014

[338] Also see Article 17 of the Data Protection Regulation

[339] Z. Akhtar, Malicious communications, media platforms and legal sanctions, 20(6) *Computer and Telecommunications Law Review* 2014, 179-187, 186

[340] Article 80 of the Data Protection Regulation; ibid (Akhtar) 186

whilst cyber attacks have to be reported under the Network and Information Security Directive 2016/1148.[341]

The European Union has been proactive in combating cybercrime through a host of different measures, which are primarily focused on protecting and securing digital data as well as retaining and processing data and when cyber-criminals are being prosecuted, it is also important to regulate to which extent this data can constitute admissible evidence in criminal proceedings.

[341] C. Walker, EU rules on breach notification, Olswang, 2014 <http://www.olswang.com/articles/2014/06/eu-rules-on-breach-notification/> accessed 1 July 2014

1.11 Surveillance Laws in the UK

Surveillance can be defined as the "*observation and collection of data to provide evidence for a purpose."*[342] It is possible to distinguish internet from electronic surveillance and the former takes place when data or content is being intercepted over the internet, whereas the latter takes place when electronic devices are used to listen, record, monitor and store communications covertly.[343] Gillespie (2009) explains that internet surveillance can denote investigating what persons do online or employing online methods to conduct offline surveillance, for instance, by using a device on a car which connects to the internet.[344] Internet surveillance can be conducted, for instance, by examining web postings, web usage and persons' online relationships.[345] In recent times, Sarfaraz (2014) notes that governments have increasingly used surveillance programs to ensure security and combat terrorism and these government surveillance programs can capture a broad spectrum of data, as individuals increasingly use digital devices on which they store personal information, such as mobile phones, laptops and other electronic gadgets.[346] However, as observed by the UK House of Lords Select Committee on the Constitution *"the role of technology in surveillance is pre-eminent and poses formidable regulatory problems"*, particularly since surveillance conflicts with fundamental rights, particularly the right to privacy and also freedom of expression

[342] Black's Law Dictionary <http://thelawdictionary.org/> accessed 20th January 2015; cited from H. Sarfaraz, Surveillance, privacy and cyber law, 20(7) *Computer and Telecommunications Law Review* 2014, 189-194, 189
[343] H. Sarfaraz, Surveillance, privacy and cyber law, 20(7) *Computer and Telecommunications Law Review* 2014, 189-194, 189
[344] A. A. Gillespie, Regulation of internet surveillance, 4 *European Human Rights Law Review* 2009, 552-565, 552
[345] Ibid
[346] H. Sarfaraz, Surveillance, privacy and cyber law, 20(7) *Computer and Telecommunications Law Review* 2014, 189-194, 189

and results in a lot of control which can be abused by those in power and this can undermine democracy and the rule of law.[347]

Gersch (2012) explicates that historically the state conducted intercepts and covert surveillance under the royal prerogative and telephone calls could be tapped and recorded to prevent or detect crime by virtue of s.80 of the Post Office Act 1969 and whilst the latter was unsuccessfully challenged in *Malone v Metropolitan Police Commissioner (No.2),*[348] the European Court of Human Rights later found that there existed confidentiality when persons use telephones. [349] The Interception of Communications Act 1985 subsequently permitted the police the power to intercept when a warrant had been issued and thus spelt out a regime to ensure that telecommunications systems were only lawfully intercepted in certain situations.[350] A tribunal was also established where complaints could be lodged about unlawful interception of communications and the Interception of Communications Commissioner was appointed to monitor intercepts.[351]

Mobbs (2003) explains that the powers to conduct direct surveillance were modernised and increased by virtue of the Regulation of Investigatory Powers Act 2000 (RIPA), as well as the Terrorism Act 2000, which allow governmental agencies to tap the networks

[347] Select Committee on the Constitution, Second Report of Session 2008-09: Surveillance: Citizens and the State, House of Lords Paper No.18-I. (Session 2008-09) 1-130, para.43 <http://www.publications.parliament.uk/pa/ld200809/ldselect/ldconst/18/18.pdf> accessed 20th January 2015; cited from A. A. Gillespie, Regulation of internet surveillance, 4 *European Human Rights Law Review* 2009, 552-565, 552
[348] [1979] Ch 344
[349] *Malone v United Kingdom* (A/82) (1985) 7 EHRR 14
[350] A. Gersch, Covert surveillance - a snoopers' charter? *Archbold Review* 2012, 5-8, 5-6
[351] Ibid, 6

and communications of individuals and organisations, so long as this has been authorised by a person with the power to do so.[352] Newburn and Neyroud (2013) inform that RIPA not only substituted the Interception of Communications Act 1985, but also changed Part III of the Police Act 1997 and the Intelligence Services Act 1994 and is supplemented by several codes of practice, such as the Covert Surveillance Code and the Covert Human Intelligence Sources Code, which had to be issued by virtue of sections 71-72 of RIPA.[353] RIPA also replaces the Complaints Tribunal with the Investigatory Powers Tribunal (IPT).[354]

Goold (2009) observes that RIPA was primarily enacted to ensure that surveillance activities would not violate the Human Rights Act 1998 and to prevent challenges to policing powers, as happened for instance in *Halford v United Kingdom*[355] and *Khan v United Kingdom*[356] and the reform was only minimal.[357] The adoption of the RIPA was nonetheless extremely important.

In *R v Khan,*[358] Lord Nolan of the House of Lords explains that *"[t]he sole cause of this case coming to your Lordship's House is the lack of a statutory system regulating the use of surveillance devices by the police. The absence of such a system seems astonishing, the more so in view of statutory framework which has governed the use of*

[352] P. Mobbs, Privacy and Surveillance, How and when organisations and the state can monitor your actions, GreenNet Civil Society Internet Rights Project, 2003, 1-11, 5 <http://www.internetrights.org.uk/briefings/irtb05-rev1-draft.pdf> accessed 29 June 2014
[353] T. Newburn, P. Neyroud, *Dictionary of Policing* (Willan Publishing 2013) 238
[354] A. Gersch, Covert surveillance - a snoopers' charter? *Archbold Review* 2012, 5-8, 6
[355] (1997) 24 E.H.R.R. 523 ECtHR
[356] (2001) 31 E.H.R.R. 45 ECtHR
[357] B. Goold, Liberty and others v The United Kingdom: a new chance for another missed opportunity, *Public Law* 2009, 5-14, 5
[358] (1997) AC 558, at 570

such devices by the Security Service since 1989, and the interception of communications by the police as well as by other agencies since 1985."[359]

Yet Goold (2009) considers that even the modernised surveillance regime adopted by RIPA - *"while detailed and far-reaching - is riddled with gaps and lacks any clear set of overarching legal principles or common objectives"* and gives as example that there are four different statutory regulators: the Interception of Communications Commissioners, the Surveillance Commissioner, the Information Commissioner and the Intelligence Services Commissioner which all deal with overlapping subject matters, but without close coordination between the different regulators, so that as a result the various regulatory frameworks are not harmonised.[360] In this context, the Joint Committee on Human Rights (2005) also notes that *"there is a mish-mash of oversight arrangements"* and that this is problematic since this disjointed approach erodes important "*counter-balancing safeguards"* and it is unclear to which extent these Commissions have the necessary resources, so that it is difficult for the Commissioners to fulfil their respective role of providing scrutiny.[361]

Furthermore, it has been observed that *"RIPA is a convoluted piece of legislation"*, for instance, because it *"is not a complete regulatory code"*, only amends *"Part III of the*

[359] Also see N. Jarvie, Control of cybercrime - is an end to our privacy on the Internet a price worth paying? Part 2, 9(4) *Computer and Telecommunications Law Review* 2003, 110-115, 113
[360] B. Goold, Liberty and others v The United Kingdom: a new chance for another missed opportunity, *Public Law* 2009, 5-14, 6
[361] Joint Committee on Human Rights, *Counter-Terrorism Policy and Human Rights: Terrorism Bill and related matters, Third Report of Session 2005-2006, Volume II-Oral and Written Evidence* (London, Stationery Office 2005) 159

Police Act 1997 and...the Intelligence Services Act 1994."[362] Moreover, Gillespie (2009) observes that RIPA only partially defines surveillance to include:[363]

> *"a) monitoring, observing or listening to persons, their movements, their conversations or their other activities or communications;*
> *(b) recording anything monitored, observed or listened to in the course of surveillance; and*
> *(c) surveillance by or with the assistance of a surveillance device."*[364]

Jarvie (2003) explains that Part I of RIPA deals with acquiring and disclosing communications data, Part II sets out how covert human intelligence sources and surveillance are regulated and Part II spells out powers, so that private encryption keys can be disclosed.[365]

The human rights advocacy group Liberty (2010) explains that RIPA applies to five kinds of surveillance[366]: Firstly, "*interception of communications"*, which normally includes emails and telephones and requires an interception warrant. Secondly, *"intrusive surveillance"*, which means bugging a house or car or filming a person, though in some instances, this is also covered by Part 3 of the Police Act 1997 and s.5 of

---

[362] Editorial, Admissibility; Criminal evidence; Privacy; Surveillance; Telecommunications, Criminal Law Review 2000, 877-878, 877-878
[363] A. A. Gillespie, Regulation of internet surveillance, 4 *European Human Rights Law Review* 2009, 552-565, 553-554
[364] S.48(2) of RIPA
[365] N. Jarvie, Control of cybercrime - is an end to our privacy on the Internet a price worth paying? Part 2, 9(4) *Computer and Telecommunications Law Review* 2003, 110-115, 110
[366] Liberty, Summary of Surveillance Powers Under RIPA, 2010, 1-17, 1 <http://www.liberty-human-rights.org.uk/materials/introduction-to-ripa-august-2010.pdf> accessed 29 June 2014

the Intelligence Services Act 1994 and again this requires authorisation. Thirdly, *"directed surveillance"* is predominantly conducted in public spaces, often with the objective to gather information about the private life of a person and again this necessitates authorisation. Fourthly, *"covert human intelligence sources"* are persons, who gather information by forming a relationship in order to gather information and are guided by a public authority. Fifthly, *"communications data"* means recording communications, whether about webpages visited, emails, telephone calls and three types of data are included, namely *"traffic data"*, *"service use"*, *"subscriber information"*,[367] but not the content and pursuant to RIPA there are three types of data: subscriber information (s.21(4)(c) of RIPA), service-use data (S.21(4)(b) of RIPA) and traffic data (S.21(4)(a) and (6) of RIPA).[368]Akhtar (2014) corroborates that s.8(1) of RIPA makes clear that a specific warrant has to be issued when internal communications are being monitored in respect of British residents who reside in the UK and this particular warrant should be granted when the person is suspected of illegal activity, but external communications can be monitored so long as a general warrant has been issued by virtue of s.8(4) of RIPA.[369]

Wicks and Carney (2009) further explain that RIPA distinguishes two types of surveillance: directed surveillance which is *"covert but not intrusive"* (s.26(2) of RIPA) and intrusive surveillance, which takes place when a person or listening device is used

[367] Ibid, 1-3
[368] A. A. Gillespie, Regulation of internet surveillance, 4 *European Human Rights Law Review* 2009, 552-565, 559
[369] Z. Akhtar, Malicious communications, media platforms and legal sanctions, 20(6) *Computer and Telecommunications Law Review* 2014, 179-187, 184

"on any residential premises or in any private vehicle" (s.26(3) of RIPA).[370] Different control frameworks have been established and which are detailed in Chapter II of RIPA in order to deal with these two types of surveillance and a higher degree of approval and authorisation is required from the surveillance commissioner for intrusive surveillance than in respect of covert surveillance [371] and additionally, Home Office Codes of Practice have to be adhered to. These control frameworks are internal, though subsequently the Office of Interception Commissioners can conduct a review by sampling and Akdeniz et al (2001) criticise the fact that there is only such limited scrutiny. [372] Akhtar (2014) points out that the previous Surveillance Commissioner considered that they could not properly monitor abuse in respect of intrusive powers since the intelligence which justified the intrusive powers could not be reviewed by the surveillance commissioners.[373] In the House of Lords in *Re McE,*[374] the question arose whether appellants, who were detained for terrorist related offences could be monitored whilst they saw their solicitors, whilst another saw a consultant psychiatrist. They sought an assurance from the police, but this was refused. They challenged that this breached their rights under the European Convention on Human Rights. The majority of the House of Lords decided that the right to legal professional privilege could be limited and when this was the case, this should be considered an intrusive surveillance under Part II of RIPA. Hence, an internal authorisation is insufficient in respect of privileged material. Moreover, Lord Hope explained that covert surveillance was permitted and

[370] D. Wicks, D. Carney, Covert surveillance, Case Comment, 82(2) *Police Journal* 2009, 183-186, 185
[371] Ss32 and 36-39 of RIPA
[372] Y. Akdeniz, N. Taylor and C. Walker, Bigbrother.gov.uk: state surveillance in the age of information and rights, *Criminal Law Review* 2001, 73-90, 73
[373] Z. Akhtar, Malicious communications, media platforms and legal sanctions, 20(6) *Computer and Telecommunications Law Review* 2014, 179-187, 184
[374] [2009] UKHL 15

that the powers under RIPA made it possible to limit the right to privacy and resultantly private consultations were not immune, so long as the conditions in RIPA were satisfied.

In terms of the criteria, Gillespie (2009) explains that for directed surveillance, this has to take place covertly, there has to be a particular operation or a particular investigation, the purpose has to be to collect private information and the operation cannot be undertaken in response to an immediate situation.[375] This suggests that directed surveillance cannot be carried out for a routine operation. The ACPO has stated that one key principle is that *"[a]uthorisation under the Regulation of Investigatory Powers Act 2000 is not necessary in order to browse the World Wide Web as part of a specific operation or investigation."*[376] Clearly, adopting such an approach is important to effectively police the digital realm.

Additionally, RIPA has provisions, which allow delegated legislation to be passed. Gersch (2012) explains that this is rather controversial since as a result of this, 792 different agencies made use of RIPA by 2008, including local authorities, the Royal Pharmaceutical Society and several other bodies.[377] For instance, in *Paton v Poole Burgh Council,*[378] five complaints were brought against Poole Borough Council, which had relied on RIPA to conduct surveillance in order to ascertain whether Ms Paton had provided the correct address for a particular catchment area of a school for her child and the Council argued that surveillance was necessary in such an instance *"for the purpose*

[375]Ibid, 537
[376]Cited from ibid, 557-558
[377] A. Gersch, Covert surveillance - a snoopers' charter? *Archbold Review* 2012, 5-8, 6
[378] Unreported July 29, 2010 (IPT)

of preventing or detecting crime." However, no criminal offence was committed for falsely stating the wrong address, apart from not being provided with a place in a school, so that the Council failed to establish that the activity fell within the scope for which surveillance was lawful, also because the Council had failed to consider whether it was reasonably necessary to conduct surveillance.[379]

The above case illustrates situations where surveillance may be considered disproportionate. On this matter, Lady Manningham-Buller, the former head of MI5, shared her reservations:

> *"[w]hen RIPA was introduced ... I assumed wrongly that the activities authorised by that legislation would be confined to the intelligence and security agencies, the police, and Customs and Excise. The legislation was drafted at the urgent request of the intelligence and security community so that its techniques would be compatible with the Human Rights Act when it came into force in 2000. I can remember being astonished to read that organisations such as the Milk Marketing Board, and whatever the equivalent is for eggs, would have access to some of the techniques. On the principle governing the use of intrusive techniques which invade people's privacy, there should be clarity in the law as to what is permitted and they*

[379] Also see Case Comment, Unlawful directed surveillance, 15(4) *Communications Law* 2010, 122-123, 122-123

should be used only in cases where the threat justified them and their use was proportionate."[380]

Apart from the great number of agencies which can make use of RIPA and the disagreement whether authorisation is required for directed surveillance, Ramraj et al (2005) further explicate that authorisation is too wide since it can be granted for very far-reaching reasons:[381] to protect national security, to avert and identify serious crime, to prevent disorder, to protect the economic prosperity of the UK or the UK economic interests, to render assistance under an agreement with another country, in the name of public safety, public health and to determine and gather tax.[382] However, the House of Lords also held in *Re C's Application for Judicial Review*,[383] that the statutory and common law right to seek privately legal advice or consult a medical professional could be qualified under RIPA and covert surveillance could take place, in this case in a prison or in a police station when a person seeks advice from a medical professional or lawyer. So long as this was labelled intrusive directed surveillance and the more stringent protective safeguards were applied, this was considered permissible. Such approach benefits law enforcement agents, as they are given broad powers to conduct surveillance, which is invaluable in order to secure the digital realm; and like the UK, the UAE also undertakes surveillance.

---

[380] Baroness Manningham-Buller, Col.297, Parliament.co.uk, 9 December 2008 <http://www.publications.parliament.uk/pa/ld200809/ldhansrd/text/81209-0006.htm#08120935000423> accessed 20th January 2015; cited from A. Gersch, Covert surveillance - a snoopers' charter? *Archbold Review* 2012, 5-8, 6

[381] V. V. Ramraj, M. Hor, K. Roach, *Global Anti-Terrorism Law and Policy* (Cambridge, Cambridge University Press 2005) 217

[382] Liberty, Summary of Surveillance Powers Under RIPA, 2010, 1-17, 16 <http://www.liberty-human-rights.org.uk/materials/introduction-to-ripa-august-2010.pdf> accessed 29 June 2014

[383] [2009] UKHL 15; [2009] 1 AC 908

1.12 Surveillance Laws in the UAE

The UAE has been filtering web sites in order to identify unlawful contents, for instance, pornography, drug use and gambling.[384] Al Lawati (2011) notes that this activity has been undertaken quite stringently, to the extent that Reporters Without Borders have labelled *"the UAE as being 'under surveillance.'"*[385] Jones (2010) also reports that the government has got the capacity to monitor internet use.[386] The non-governmental organisation Freedom House (2013) reports that the UAE's commitment to achieving a safe digital space is underscored by the fact that it reached the 28th place in the United Nations 2012 E-Governance Survey and the 25th on the World Economic Forum's 2013 Networked Readiness Index Freedom.[387] The cybercrime units in co-operation with the Telecommunications Regulatory Authority are entrusted with *"tracking cyber-criminals"*, whilst the department of anti-electronic crimes was formed at the Dubai investigation department.[388] In an interview with Reporters without Borders, Major Salem Obaid Salmeen (2014) explained that *"These electronic patrols are detecting and tracking all topics and materials written and presented on these*

[384] OpenNet Initiative, Internet Filtering in the United Arab Emirates in 2006-2007, 2007 <https://opennet.net/studies/uae2007> 30 June 2014
[385] A. Al Lawati, UAE internet policies put under the microscope, Gulfnews, 2011 <http://gulfnews.com/news/gulf/uae/media/uae-internet-policies-put-under-the-microscope-1.765600> accessed 30 June 2014
[386] S. Jones, Global Dispatches: UAE - A Guide for Internet Use in the UAE, The Epoch Times, 2010 <http://www.theepochtimes.com/n2/opinion/uae-internet-united-arab-emirates-blckberry-google-government-42724.html> accessed 30 June 2014
[387] Freedom House, United Arab Emirates 2013 <http://www.freedomhouse.org/report/freedom-net/2013/united-arab-emirates#.U7XAKECmWMY> accessed 30 June 2014
[388] Reporters without Borders, United Arab Emirates: Tracking "cyber-criminals", 2014 <http://12mars.rsf.org/2014-en/2014/03/11/united-arab-emirates-tracking-cyber-criminals/> accessed 30 June 2014

websites...Dubai's police is equipped with the latest technologies in the field and has a qualified team specializing in anti-electronic crimes..."[389] The Telecommunications Regulatory Authority blocks the following seven different types of websites: websites with content which contravene UAE morals and ethics, which express religious hatred, which contravene UAE laws, which permit users to read blocked content, which constitutes a risk to internet users, for instance, phising websites and, for instance, those websites which allow gambling or offer illegal drugs.[390]

Mustafa (2014) reports that as of 2014 the UAE doubled its security budget, from $5.5 billion to $10 billion,, and that a large part of it was planned to be used to strengthen cyber-security.[391] Aleksander Mitreski (2014) of INEGMA notes that *"the investment is likely to be into surveillance and communications monitoring..[to] provide a full spectrum of communications, surveillance and analytics."*[392] Yet the surveillance has to be put on a statutory footing, as currently only Article 43 of the Federal Legal Decree No. 5 for 2012 mentions surveillance of those, who have been prosecuted, but this does not promote a proactive policing approach towards cybercrime. There is also no mention of data retention, despite being a very important aspect, which the UK and Europe have addressed, as discussed next.

[389] Ibid
[390] Ibid
[391] A. Mustafa, UAE to Double Security Budge, Focus on Cyber, Defense News, 2014 <http://www.defensenews.com/article/20140224/DEFREG04/302240015/UAE-Double-Security-Budget-Focus-Cyber> accessed 30 June 2014
[392] Cited from ibid

1.13 The UK and European Approach Towards Data Retention

Bernal (2014) explains that data retention laws generally require those who already collect data to keep it and share it.[393] Jewkes and Mar (2011) corroborate that following 9/11, the UK government requested the telecommunication sector and internet service providers in 2003, pursuant to Part II of the Anti-Terrorism Crime and Securities Act 2001, to voluntarily retain data for six months, though web server logs had to only be kept for up to four days.[394] The Secretary of State could also make an order to render the voluntarily obligation legally binding if this was required.[395]

Certainly, data retention is as such not unlawful, for instance, when there is a *"serious threat to public safety posed by organised terrorism in the United Kingdom"*, as explained by the European Court of Human Rights in *McVeigh, O'Neill and Evans v United Kingdom.* [396] Taylor (2003) explicates that the Anti-Terrorism, Crime and Security Act 2001 also allows that communications data can be retained and extensive information about the private life of a person can thereby be obtained.[397] Equally, legislation, such as RIPA, can be used to access retained data. [398]

Konstadinides (2011) explains that following the Madrid bombings in 2004 and the London attacks in 2005, there was a pressing need to exercise control in respect of telecommunications within Europe, as this would help with preventing, investigating,

[393] P. Bernal, *Internet Privacy Rights: Rights to Protect Autonomy* (Cambridge University Press 2014) 103
[394] Y. Jewkes, M. Yar, *Handbook of Internet Crime* (Abingdon, Willan Publishing 2011) 427
[395] Ibid
[396] (1981) 5 EHRR 71; N. Taylor, Policing, privacy and proportionality, *European Human Rights Law Review* 2003, 86-100, 96
[397] Ibid (Taylor) 97
[398] P. Bernal, *Internet Privacy Rights: Rights to Protect Autonomy* (Cambridge University Press 2014) 104

detecting and prosecuting terrorists and organised criminals.[399]Jewkes and Mar (2011) point out that data retention has therefore been dealt with at the European level.[400] Equally, Konstadinides (2011) explains that this is because European criminal law has developed and EU mechanisms have thus been adopted to ensure access, data collection and also exchange of data.[401] This necessitates that private and public bodies cooperate with each other.[402]

Walker (2011) notes that initially, the European Union Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector was adopted and Article 15 particularly allowed for data retention for some time to protect *"national security, defence, public security or the prevention, investigation, detection, and prosecution of criminal offences of unauthorised use of the electronic communications system."*[403] Subsequently, Directive 2006/24/EC on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC (the Data Retention Directive) was adopted, resulting in harmonised data retention of between 6 and 24 months in the European Union.[404] This Directive permitted that individual data could be used when investigating, detecting and prosecuting serious crime in accordance with the definition adopted by the domestic law of the Member States and removed regulatory

[399] T. Konstadinides, Destroying democracy on the ground of defending it? The Data Retention Directive, the surveillance state and our constitutional ecosystem, 36(5) *European Law Review* 2011, 722-736, 724
[400] Y. Jewkes, M. Yar, *Handbook of Internet Crime* (Abingdon, Willan Publishing 2011) 427-428
[401] T. Konstadinides, Destroying democracy on the ground of defending it? The Data Retention Directive, the surveillance state and our constitutional ecosystem, 36(5) *European Law Review* 2011, 722-736, 722
[402] Ibid, 723
[403] C. Walker, *Terrorism and the Law* (Oxford, Oxford University Press 2011) 75
[404] Y. Jewkes, M. Yar, *Handbook of Internet Crime* (Abingdon, Willan Publishing 2011) 427-428

dissimilarities in respect of electronic communications which impeded the internal market.[405]Pursuant to the Directive, listed providers had to retain location and traffic data and related data which was needed to identify users or subscribers, though this did not extend to retaining information which had been consulted or the content.[406]

The UK adopted the Data Retention Directive by virtue of the Data Retention (EC Directive) Regulations 2007 (SI 2007/2199).[407] The Explanatory Memorandum of the Regulations states that *"this valuable data has allowed investigators to identify suspects, examine their contacts, establish relationships between conspirators and place them in a specific location. Communications data is used in numerous other ways, including assisting investigation of suspects' interaction with victims and in support of suspects' alibi."*[408] In the UK, the Regulations 2007 were replaced by the Data Retention (EC Directive) Regulations 2009, so that data from email, internet telephony and internet access is included and has to be retained across the board for 12 months, except where the provider has been requested to retain the data longer by virtue of the 2009 Regulations.[409] The Committee on the Internal Market and Consumer Protection for the Committee on Civil Liberties, Justice and Home Affairs (2005) noted that the Data Retention Directive has resulted in "a paradigm shift in the way society looks at traffic data."[410] Salgado (2014) also notes that the adoption of the Data Retention Directive was

[405] T. Konstadinides, Destroying democracy on the ground of defending it? The Data Retention Directive, the surveillance state and our constitutional ecosystem, 36(5) *European Law Review* 2011, 722-736, 727
[406] Case Comment, Data retention Directive invalid, says ECJ, 319 *EU Focus* 2014, 14-16, 14-15
[407] Cited from C. Harding, K. Harfield, *Covert Investigation* (3rd edn, Oxford, Oxford University Press 2012) 104
[408] Ibid
[409] C. Walker, *Terrorism and the Law* (Oxford, Oxford University Press 2011) 75
[410] Opinion of the Committee on the Internal Market and Consumer Protection for the Committee on Civil Liberties, Justice and Home Affairs on the proposal for a directive of the European Parliament and of the

controversial since it effectively permitted "blanket government surveillance on communications data."[411]

This was particularly the case since the European Commission did not consider it necessary to adopt any protective safeguards against possible abuses in respect of traffic communications data retention and stated that *"specific additional provisions on general data protection principles and data security are not necessary."*[412] Hence, the Data Protection Directive contained no such provisions. Salgado (2014) further explicates that the Data Retention Directive, whilst providing that data retention is only permissible for investigating, detecting and prosecuting serious crime and sharing it with competent authorities, failed to define what constitutes a serious crime (apart from the recitals of the Directive referring to organised crime and terrorism) and competent authorities and also did not clarify what data sharing procedures should be used and all this was left up to the Member States.[413]

The European Data Protection Supervisor perceived such an approach as flawed and therefore noted that *"a simple reference to the existing legal framework on data*

Council on the retention of data processed in connection with the provision of public electronic communication services and amending Directive 2002/58, COM(2005) 0438 -- C6-0293/2005 -- 2005/0182 (COD); T. Konstadinides, Destroying democracy on the ground of defending it? The Data Retention Directive, the surveillance state and our constitutional ecosystem, 36(5) *European Law Review* 2011, 722-736, 727

[411] M. Salgado, Data retention - what now? 14(7) *Privacy & Data Protection* 2014, 13-14, 13-14

[412] European Commission Proposal COM(2005) 438 final, Retention of data processed in connection with the provision of public electronic communication services, 1-17, 3 <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2005:0438:FIN:EN:PDF> accessed 20th January 2015; cited from T. Konstadinides, Destroying democracy on the ground of defending it? The Data Retention Directive, the surveillance state and our constitutional ecosystem, 36(5) *European Law Review* 2011, 722-736, 726

[413] M. Salgado, Data retention - what now? 14(7) *Privacy & Data Protection* 2014, 13-14, 13

protection (in particular the Directives 95/46/EC and 2002/58/EC) was not sufficient."[414]

Equally, the European Economic and Social Committee observed that it is likely that the Directive will be found unconstitutional by domestic courts since the approach to safeguard fundamental rights is too weak and the European Parliament Minority Opinion (2005) shared this view and considered that the time for which data has to be retained is too long.[415]

Similarly, Walker (2011) questions whether this *"indiscriminate interference with private information is necessary and proportionate within Article 8(2)"* of the European Convention on Human Rights, the latter Article guaranteeing the right to privacy, as further discussed below.[416] In this context, Article 2(1) of the Council of Europe Recommendation No. R (87) 15 regulating the use of personal data in the police sector (1987) is also noteworthy since it states that personal data should only be gathered to the

[414] Opinion of the European Data Protection Supervisor on the proposal for a Directive of the European Parliament and of the Council on the retention of data processed in connection with the provision of public electronic communication services and amending Directive 2002/58 [2005] OJ C298/1 <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2005:298:0001:0012:EN:PDF> accessed 20th January 2015; European Commission Proposal COM(2005) 438 final, Retention of data processed in connection with the provision of public electronic communication services, 1-17 <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2005:0438:FIN:EN:PDF> accessed 20th January 2015; cited from T. Konstadinides, Destroying democracy on the ground of defending it? The Data Retention Directive, the surveillance state and our constitutional ecosystem, 36(5) *European Law Review* 2011, 722-736, 727

[415] Opinion of the European Economic and Social Committee on the Proposal for a Directive of the European Parliament and of the Council on the retention of data processed in connection with the provision of public electronic communication services and amending Directive 2002/58 COM(2005) 438 final--2005/0182 (COD);European Parliament, Minority Opinion pursuant to Rule 48(3) of the Rules of Procedure, A6-0365/2005 final, Report on the proposal for a directive of the European Parliament and of the Council on the retention of data processed in connection with the provision of public electronic communication services and amending Directive 2002/58/EC (COM(2005)0438) - C6-0293/2005 - 2005/0182(COD), 28 November 2005, 1-66 <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A6-2005-0365+0+DOC+PDF+V0//EN> accessed 20th January 2015; cited from ibid (Konstadinides) 727

[416] C. Walker, *Terrorism and the Law* (Oxford, Oxford University Press 2011) 75

extent that this is necessary to prevent particular criminal offences or to avert real danger and that exceptions to this should be clearly spelled out by domestic legislation.[417] However, the Economic Crime Division of the Council of Europe (2008) points out that currently domestic legislation does not draw a distinction between criminal offences, surveillance or security investigation and that also different groups of data are not distinguished, for instance, *"investigative (police) data"*, which is also important to adhere to the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data.[418] However, Cannataci (1987) corroborates that the recommendation is not binding[419] and equally Boehm (2012) points out that *"the binding force of [the Recommendation and Convention] might be controversial."*[420]

Konstadinides (2011) highlights that the Data Retention Directive raises thorny issues since *"[r]etaining communication and location data of all citizens in the European Union has raised sensitive issues related to the far-reaching impact of EU harmonisation legislation on privacy and the protection of personal data"* and strong legal safeguards should be therefore adopted to prevent abuse and to ensure that the

[417] Also see Council of Europe, Economic Crime Division, Cybercrime investigation and the protection of personal data and privacy, 2008, 1-52 <http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/documents/reports-presentations/567%20study5-d-provisional.pdf> accessed 30 June 2014

[418] Ibid

[419] J. A. Cannataci, Study on Recommendation No. R (87) 15 of 17 September 1987 regulating the use of personal data in the police sector, "Data Protection Vision 2020, Options for improving European policy and legislation during 2010-2020, Strasbourg, 2010, 1-88, 6 <http://www.coe.int/t/dghl/standardsetting/dataprotection/J%20A%20Cannataci%20Report%20to%20Council%20of%20Europe%20complete%20with%20Appendices%2031%20Oct%202010.pdf> accessed 1 July 2014

[420] F. Boehm, *Information Sharing and Data Protection in the Area of Freedom, Security and Justice, Towards Harmonised Data Protection Principles for Information Exchange at EU-level* (London, Springer 2012) 96

rights in Article 16 of the TFEU, the European Convention on Human Rights (ECHR) and the EU Charter of Fundamental Rights are not undermined.[421] Equally, Bernal (2014) notes that the issue with the Data Retention Directive is that authorities may gather too much data.[422] However, Harding and Harfield (2012) emphasise that when combating cybercrime, communications data can prove invaluable to identify patterns and criminal links and can help with prosecutions or with deciding whether or not more intrusive surveillance should be undertaken.[423] In contrast, Konstadinides (2011) considers that following the Data Retention Directive *"[m]ere suspicion suffices to resort to actions, such as intense and all-encompassing telecommunications surveillance, bringing Member States close to the pervasive Orwellian 'surveillance state' model."*[424] The danger is that innovation within information-delivery systems and large databases can assist authoritarian regimes to quell oppositions.[425] It also leads to democratic states eroding fundamental rights and human rights and this may undermine the very foundation on which democracy and the rule of law is based, particularly if insufficient safeguards and checks and balances are implemented and stringently

[421] Article 16 of the TFEU states
1. Everyone has the right to the protection of personal data concerning them.
2. The European Parliament and the Council, acting in accordance with the ordinary legislative procedure, shall lay down the rules relating to the protection of individuals with regard to the processing of personal data by Union institutions, bodies, offices and agencies, and by the Member States when carrying out activities which fall within the scope of Union law, and the rules relating to the free movement of such data. Compliance with these rules shall be subject to the control of independent authorities.
The rules adopted on the basis of this Article shall be without prejudice to the specific rules laid down in Article 39 of the Treaty on European Union"; T. Konstadinides, Destroying democracy on the ground of defending it? The Data Retention Directive, the surveillance state and our constitutional ecosystem, 36(5) *European Law Review* 2011, 722-736, 723
[422] P. Bernal, *Internet Privacy Rights: Rights to Protect Autonomy* (Cambridge University Press 2014) 104
[423] C. Harding, K. Harfield, *Covert Investigation* (3rd edn, Oxford, Oxford University Press 2012) 104
[424] T. Konstadinides, Destroying democracy on the ground of defending it? The Data Retention Directive, the surveillance state and our constitutional ecosystem, 36(5) *European Law Review* 2011, 722-736, 724
[425] US National Intelligence Council, *Global Trends 2030: Alternative Worlds* (Washington DC, US Government Printing Office 2012) 88

enforced.[426] Hence, those who can access and use the new wealth of data about individuals should also be stringently enforced to counter the risk of an emergence of the Orwellian state.[427]

In *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources*[428], the Grand Chamber of the Court of Justice of European Union (CJEU) found that the Data Retention Directive was invalid and illegal since fundamental rights were being breached in respect of private life, and personal data was insufficiently protected since the situations in which authorities could access information were not adequately restricted.[429] Torremans (2014) points out that the court considered that there was far-reaching and particularly grave interference with Articles 7 and 8 of the EU Charter of Fundamental Rights which affirm the rights to respect for private life and communications and the protection of personal data and this interference was inconsistent with the EU principles of necessity, as well as proportionality.[430] Hopkins (2014) observes that virtually *"the entire European population"* had their fundamental rights interfered with.[431] As a result, the Directive was considered invalid from its inception.[432] The following five particular shortcomings were identified within the Directive by the Grand Chamber: Firstly, all persons, all traffic data and all

[426] Ibid
[427] Ibid
[428] (C-293/12) [2014] 3 W.L.R. 1607 (ECJ (Grand Chamber))
[429] Also see Case Comment, Uncertainty for EU ISPs as court declares retention law invalid, 14(5) Privacy & Data Protection 2014, 1, 17, 1; Case Comment, Data Retention Directive is declared invalid by ECJ, 19(2) *Communications Law* 2014, 38
[430] P. Torremans, *Research Handbook on Cross-border Enforcement of Intellectual Property* (Cheltenham, Edward Elgar Publishing Ltd 2014) 303
[431] R. Hopkins, Interfering with the fundamental rights of practically the entire European population, Panopticon, 10th April 2014 <http://www.panopticonblog.com/2014/04/10/interfering-with-the-fundamental-rights-of-practically-the-entire-european-population/> accessed 21st August 2015
[432] Case Comment, Data retention Directive invalid, says ECJ, 319 *EU Focus* 2014, 14-16, 15

communications are covered and no limitation is imposed; secondly, no criteria are stipulated which domestic enforcement agencies have to make out to access data and equally no limitations are specified; thirdly, the periods for which data can be retained make no distinction in respect of the types of data in relation to the particular persons or the kind of investigation and the retention period is not limited to a necessary period; fourthly, there are no adequate safeguards to prevent that data is being abused or unlawfully accessed or used; fifthly, data does not have to be kept within the EU and resultantly insufficient control is exercised over the data.[433] The decision cannot be appealed by the European Commission, though a new law can be proposed, but it may take years to adopt one.[434] Salgado (2014) observes that the fact that the CJEU requires data to be kept within the European Union, may also cause problems, as very often global companies offer electronic communications services and which use cloud computing, so that such a restriction may impede economic and technological development.[435] However, fundamentally the CJEU did not rule that data retention is unlawful per se, especially since the Directive does not permit that the content of communications can be acquired and also because data retention can be justified to be in the general interest and the issue with the Directive is that it failed to spell out the scope and extent to which an interference is permissible, as the scope of the data which can be retained is too wide, there is no relation between the communications data which is being retained and the public security threat, there are no criteria which competent authorities have to satisfy to access retained data, the different periods to retain data

[433] Case Comment, Uncertainty for EU ISPs as court declares retention law invalid, 14(5) Privacy & Data Protection 2014, 1, 17, 17
[434] Ibid
[435] M. Salgado, Data retention - what now? 14(7) *Privacy & Data Protection* 2014, 13-14, 14

have no criteria for a specific period, no safeguards have to be satisfied by providers which retain data and the data does not have to be stored within the EU.[436] As a corollary, if these issues were rectified, data retention would be legal and not considered invalid.

In response to the decision, the UK Home Office also stated *"We are considering the judgment and its implications carefully. The retention of communications data is absolutely fundamental to ensure law enforcement have the powers they need to investigate crime, protect the public and ensure national security."*[437] Salgado (2014) observes that the issue is that Member States, like the UK, which have transposed the Directive, have to change their laws and criminal convictions may even be challenged in case reliance is placed on retained data.[438] Bernal (2014) notes that this is also why the UK government introduced the Communications Data Bill (now enacted as Investigatory Powers Act 2016).[439] The Investigatory Powers Act 2016 replaced the Data Retention (EC Directive) Regulations 2009 and a targeted approach would have to be employed when data is being retained and surveillance powers are used.[440] It has extended the powers further by allowing wide extraterritorial communication acquisition and interception powers, including in respect of communications content.[441]

---

[436] Ibid
[437] Cited from Case Comment, Uncertainty for EU ISPs as court declares retention law invalid, 14(5) Privacy & Data Protection 2014, 1, 17, 17
[438] M. Salgado, Data retention - what now? 14(7) *Privacy & Data Protection* 2014, 13-14, 14
[439] P. Bernal, *Internet Privacy Rights: Rights to Protect Autonomy* (Cambridge University Press 2014) 105
[440] M. Davidson, DRIP: a knee-jerk reaction to the Digital Rights Ireland Ltd decision? Blog.JustCite.com, 18 July 2014 <http://blog.justcite.com/the-drip-bill-a-knee-jerk-reaction-to-the-digital-rights-ireland-ltd-decision> accessed 20 January 2015
[441] Liberty, Privacy International, Open Rights Group, Big Brother Watch, Article 19 and English PEN briefing on the fast-track Data Retention and Investigatory Powers Bill, 2014, 1-13, 3 <https://www.liberty-human-

The human rights advocacy group Liberty (2014) therefore labelled the Investigatory Powers Act 2016 a "*snoopers charter"* and explains that communications data within the UK could be collected, retained and made available, resulting in *"private companies be[ing] called upon to orchestrate blanket collection of personal data which they have no business to retain."*[442] However, as pointed out by the UK government, *"[w]ithout action there is a serious and growing risk that crimes enabled by email and the internet will go undetected and unpunished, that the vulnerable will not be protected and that terrorists and criminals will not be caught and prosecuted."*[443]

The Data Retention and Investigatory Powers Act 2014 was temporarily adopted in order to replace the invalid UK regulations.[444] Alder (2015) explains that under the Act the Secretary of State can publish a retention notice in which the means and time are detailed and this has to be upheld by the courts.[445] It is lawful to obtain communication data for *"the economic well-being of the UK"*, though only in respect of national security, rendering it more difficult to exploit the data commercially by selling it to interested corporations and the Act may lapse if it is not renewed by September 2016.[446] Security has also been strengthened through the recent enactment of the Counter-Terrorism and Security Act 2015 since pursuant to s.21 communications data from

---

rights.org.uk/sites/default/files/Briefing%20on%20the%20Data%20Retention%20and%20Investigatory%20Powers%20Bill.pdf> accessed 19th January 2015

[442] Liberty, No Snoopers Charter, Liberty's Submission to the Joint Committee on the Draft Communications Data Bill 1-39, 1&4 <http://www.liberty-human-rights.org.uk/pdfs/policy12/liberty-submission-to-the-draft-communications-data-bill-committee-aug-2012-.pdf> accessed 29 June 2014

[443] T. May, Home Secretary, Draft Communications Data Bill, Presented to Parliament by the Secretary of State for the Home Department by Command of Her Majesty, Cm 8359, June 2012, 1-123, i <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/228824/8359.pdf> accessed 19th January 2015

[444] Out-Law.com, EU data retention rules unlawful, rules CJEU, 8 April 2014 <http://www.out-law.com/en/articles/2014/april/eu-data-retention-rules-unlawful-rules-cjeu/> accessed 23rd August 2015

[445] J. Alder, *Constitutional and Administrative Law* (10th ed, London, Palgrave MacMillan 2015) 572

[446] J. Alder, *Constitutional and Administrative Law* (10th ed, London, Palgrave MacMillan 2015) 572

which the internet address can be identified has to be retained by service providers, though not the "web logs." [447]

It should be noted that the Investigatory Powers Act has received heavy criticism and after a recent court decision the UK government must re-write the whole Act in order to make it compatible with EU law.[448]

1.14 The UK Evidence Rules on Admissibility for Criminal Proceedings

Against the background of surveillance and data retention, it is important to scrutinise in which circumstances UK evidence law considers that evidence has been obtained by illegal or unfair means, so that it cannot be relied upon in court. This is important since the adoption of a comprehensive legislative framework to combat cybercrime in the UAE has to also clearly spell out in which circumstances the ubiquitous digital evidence, which is particularly generated by heightened surveillance and data retention, should not be used. This reinforces the rule of law and fosters legitimacy and accountability within the administration of justice.

Gersch (2012) explains that as a result of comprehensive government communications, surveillance lawyers struggle to deal with problems pertaining to disclosure of evidence in court.[449] However, in this context it is important to stress that emerging cyber law accepts that digital evidence for the court does not consist of providing extremely technical digital forensics through technological aids, but a *"case-specific assertion of*

[447] J. Alder, *Constitutional and Administrative Law* (10th ed, London, Palgrave MacMillan 2015) 572
[448] The Guardian, 'UK has six months to rewrite snooper's charter, high court rules', < https://www.theguardian.com/technology/2018/apr/27/snoopers-charter-investigatory-powers-act-rewrite-high-court-rules> Accessed 23 June 2018.
[449] A. Gersch, Covert surveillance - a snoopers' charter? *Archbold Review* 2012, 5-8, 5

fact that must be probably true in order to lend support to a legal claim."[450] S.78(1) of the UK Police and Criminal Evidence Act 1984 entitled *"exclusion of unfair evidence"* states:

> *"In any proceedings the court may refuse to allow evidence on which the prosecution proposes to rely to be given if it appears to the court that, having regard to all the circumstances, including the circumstances in which the evidence was obtained, the admission of the evidence would have such an adverse effect on the fairness of the proceedings that the court ought not to admit it."*

Accordingly, the abovementioned section confers discretion on judges to exclude evidence from the prosecution by virtue of, and as established by, the common law when unfair or illegal means have been used. This requires making recourse to Article 6 of the ECHR, which guarantees the right to a fair trial and which has to be guaranteed due to the enactment of the ECHR by virtue of the Human Rights Act 1998.[451] Prior to the Police and Criminal Evidence Act 1984, "*illegally obtained evidence was very rarely excluded."*[452] Yet as made clear by the House of Lords in *R v Khan*[453] when referring to *Schenk v Switzerland*[454] *"the European Court of Human Rights ... confirms*

[450] D. S. Schwartz, A Foundation Theory of Evidence, 100 *Georgetown Law Journal* 2011-2012, 95-172; cited from B. Longo, Learning on the wires: BYOD, embedded systems, wireless technologies and cybercrime, 13(2) *Legal Information Management* 2013, 119-123, 121
[451] A. Keane, P. McKeown, *The Modern Law of Evidence* (9th edn, Oxford, Oxford University Press 2012) 54
[452] D. Hirschel, W. Wakefield, S. Sasse, *Criminal Justice in England and the United States* (London, Jones and Bartlet Publishers 2008) 194
[453] (1996) 3 WLR 162 at 176
[454] (1997) AC 558

that the use at a criminal trial of material obtained in breach of the rights of privacy enshrined in Art.8 does not itself mean that the trial is unfair. Thus the European Court of Human Rights case law on this issue leads to the same conclusion as English law."[455] Taylor highlights that this approach raises a problem since on the one hand police behaviour has to afford certain minimum safeguards to avoid that the right to privacy is not being breached in Article 8, but because evidence can be obtained in violation of Article 8, this means that *"the standards set for policing action might be seen to be theoretical rather than practical."*[456]

As also made clear in *R v Maxwell,*[457] *"[i]t is well established that the court has the power to stay proceedings in two categories of case, namely (i) where it will be impossible to give the accused a fair trial, and (ii) where it offends the court's sense of justice and propriety to be asked to try the accused in the particular circumstances of the case. In the first category of case, if the court concludes that an accused cannot receive a fair trial, it will stay the proceedings without more. No question of the balancing of competing interests arises. In the second category of case, the court is concerned to protect the integrity of the criminal justice system. Here a stay will be granted where the court concludes that in all the circumstances a trial will 'offend the court's sense of justice and propriety' (per Lord Lowry in R v Horseferry Road Magistrates' Court, ex p Bennett [1993] 3 All ER 138, at 161, [1994] 1 AC 42 at 74) or will 'undermine public confidence in the criminal justice system and bring it into*

[455] *R v Khan* (1997) AC 558, per Lord Nicholls of Birkenhead at 583
[456] N. Taylor, Policing, privacy and proportionality, *European Human Rights Law Review* 2003, 86-100, 99
[457] [2010] UKSC 48, per Sir John Dyson SCJ

disrepute' (per Lord Steyn in R v Latif, R v Shahzad [1996] 1 All ER 353 at 360, [1996] 1 WLR 104 at 112).” The issue is that when certain policing practices become normalised, it becomes more difficult to argue that the court should stay the proceedings.

The seriousness of the offence will be considered in respect of the second consideration.[458] Whilst some exceptions exists, for instance where torture has been used,[459] in the old case of *R v Leatham*,[460] Crompton J explained that *“[i]t matters not how you get it; if you steal it even, it would be admissible in evidence”*[461] and it has been held, for example, that an invasion of privacy is not a reason to exclude.[462] Equally, in cybercrime cases it could be argued that the exclusion of retained data *“would be a dangerous obstacle to the administration of justice”*, as in the old case of *Jones v Owen,*[463] where a person was unlawfully searched, but the object was nonetheless admissible as evidence.

In *Fox v Chief Constable of Gwent*,[464] it was stated by Lord Fraser *“...if the appellant had been lured to the police station by some trick or deception, or if the police officers had behaved oppressively towards the appellant, the justices' jurisdiction to exclude otherwise admissible evidence recognised in R v Sang might have come into play....”* All the circumstances have to be therefore assessed by a judge when deciding whether to

[458] *Warren v Attorney General for Jersey* [2011] UKPC 513, 25, per Lord Dyson
[459] *A v Secretary of State for the Home Department (No.2)* [2005] 3 WLR 1249
[460] [1861] 8 Cox CC 498
[461] *R v Leatham* [1861] 8 Cox CC 498, 501
[462] *R v Khan (Sulton)* [1997] AC 558
[463] [1870] 34 JP 759
[464] [1985] 3 All ER 392

exclude evidence, as explained by Lord Lane CJ in *R v Quinn*[465] where it was stated *"The function of the judge is therefore to protect the fairness of the proceedings, and normally proceedings are fair if a jury hears all relevant evidence which either side wishes to place before it, but proceedings may become unfair if, for example, one side is allowed to adduce relevant evidence which, for one reason or another, the other side cannot properly challenge or meet, or where there has been an abuse of process, eg because evidence has been obtained in deliberate breach of procedures laid down in an official code of practice."* These procedures are contained in the Police and Criminal Evidence Act 1984 (PACE) codes of practice, which ensure that police powers are regulated, so that public rights are not abused.[466]

In the context of cybercrime this could occur in situations where no surveillance has been authorised under RIPA. Yet when there is an entrapment, then the evidence may be excluded, by virtue of s.78 or the proceedings can be struck out on the basis of an abuse of process.[467] Similarly, when undercover operations are conducted, it has to be assessed whether evidence can be excluded.[468] Nonetheless, the general principle was clearly espoused in the Privy Council case *Kuruma Son of Kaniu v R*[469] by Lord Goddard CJ, who corroborated that "In their Lordships' opinion the test to be applied in considering whether the evidence is admissible is whether it is relevant to the matters in issue. If it is, it is admissible and the court is not concerned with how the evidence was obtained.

[465] [1990] Crim LR 581
[466] Home Office, Police and Criminal Evidence Act 1984 (PACE) codes of practice, 26 March 2013 <https://www.gov.uk/guidance/police-and-criminal-evidence-act-1984-pace-codes-of-practice> accessed 1st December 2015I
[467] *R v Looseley and Attorney General's Reference (No.3 of 2000)* [2001] 1 WLR 2060
[468] *R v Smurthwaite and Gill* [1994] 1 All ER 898
[469] [1955] AC 197, 203; also see *Jeffrey v Black* [1978] QB 490

While this proposition may not have been stated in so many words in any English case there are decisions which support it, and in their Lordships' opinion it is plainly right in principle."[470] Accordingly, so long as the intercepts have been authorised, they do not breach the person's right to a fair trial guaranteed under Article 6 of the ECHR and whilst they interfere with the person's Article 8 right to privacy under the ECRH, they do not have to be excluded.[471] Hence, only when intercepts are made illegally in breach of the statute will the evidence be considered inadmissible, as for instance, in *Sargent,*[472] where the intercepts were used to obtain a confession when the person was being interviewed and the confession was then admitted as evidence,.[473]

In contrast to evidence from unlawful intercepts, under RIPA evidence from unauthorised surveillance, including intrusive surveillance, is not inadmissible, though an accused may nevertheless argue that this constitutes an abuse of process or that the judge should use s.78 of PACE.[474] This is because under Part II of RIPA, it is not rendered compulsory to obtain authorisation to undertake surveillance and no offence is committed when this happens, though enforcement agencies are best off to ensure that an authorisation has been granted to avoid that an accused arguing that his Convention rights have been breached.[475] However, a communication can also be intercepted as part

[470] Cited from R. Glover, P. Murphy, *Murphy on Evidence* (13th edn, Oxford, Oxford University Press 2013) 57
[471] *P* [2002] 1 AC 146; R. Glover, P. Murphy, *Murphy on Evidence* (13th edn, Oxford, Oxford University Press 2013) 59
[472] [2003] 1 AC 347
[473] R. Glover, P. Murphy, *Murphy on Evidence* (13th edn, Oxford, Oxford University Press 2013) 59
[474] Editorial, Admissibility; Criminal evidence; Privacy; Surveillance; Telecommunications, *Criminal Law Review* 2000, 877-878, 878
[475] Ibid

of surveillance and there is thus some overlap.[476] Generally, under RIPA evidence will be inadmissible from intercepted communication when the interception constitutes a criminal offence (ss.17 and 18 RIPA), but no criminal offence is committed when directed or unauthorised surveillance takes place and evidence is therefore not inadmissible.[477] However, the judge has to nevertheless determine how to weigh the evidence and the case of *Jones v University of Warwick*[478] is instructive, where a person was secretly filmed by an agent acting for insurers and it was found that the evidence was admissible. The court emphasised that it was warranted to inform that the insurers had behaved improperly and in an unjustified manner. Lord Woolf stated that *"[t]he fact that the insurers might have been motivated by a desire to achieve what they considered would be a just result did not justify either the commission of trespass or the contravention of the claimants privacy which took place irrespective of whether the evidence could be obtained by other means."* The court penalised this behaviour when it awarded costs.[479]

Accordingly, under RIPA, material, which has been gathered through covert surveillance, may be used in court and this can even extend to privileged conversations in case the conversations were undertaken for the purpose of fraud or crime.[480] For

[476] A. Hale, J. Edwards, Getting it taped, 12(3) *Computer and Telecommunications Law Review* 2006, 71-73, 71
[477] Ibid, 73
[478] [2003] EWCA Civ 151
[479] A. Hale, J. Edwards, Getting it taped, 12(3) *Computer and Telecommunications Law Review* 2006, 71-73, 73
[480] *R v Cox and Railton* (1884) 14 QBD 153; C's Application for Judicial Review, Re [2009] UKHL 15; [2009] 1 A.C. 908; also see D. Wicks, D. Carney, Covert surveillance, Case Comment, 82(2) Police Journal 2009, 183-186, 186

instance, in *R v Turner (Elliott Vincent)*,[481] it was held that pursuant to the Regulation of Investigatory Powers (Extension of Authorisation Provisions: Legal Consultations) Order 2010[482] surveillance could take place, even if legally privileged information[483] is thereby acquired. However, the court also cautioned that efforts should be made to maintain legal privilege, so that the investigation and trial are not tainted by unfairness and s.78 of the Police and Criminal Evidence Act 1984 cannot be evoked.[484]

It is important that the UAE also specifies the instances in which evidence should be excluded, as this will increase transparency within the administration of justice. Connected to this topic is also the question in which circumstances it should be deemed in the public interest to not disclose digital evidence.

1.14.1 The UK Evidence Rules Governing Circumstances of Public Policy Non-Disclosure

As cybercrime works includes sensitive public security areas, it is important that evidence is not admissible when this is in the public interest. In this context, sensitive evidence means *"that which the prosecution considers should not be disclosed to the defence because it would constitute a real risk of serious prejudice to an important public interest', and the prosecution do not have to produce sensitive computer evidence to the defence because 'the entitlement to disclosure of relevant evidence is not an*

[481] [2013] EWCA Crim 642
[482] (SI 2010/461)
[483] See s.98 of the Police Act 1997
[484] A. Roberts, Case Comment, R. v Turner (Elliott Vincent): evidence - surveillance, 12 *Criminal Law Review* 2013, 993-995, 994

absolute right."[485] Keane and McKeown (2012) explain that despite the principle that police sources shall not be disclosed being firmly established, the courts have only recently dealt with the matter under the public immunity doctrine.[486] Yet Phillips J in *R v Clowes*[487] acknowledged that it is difficult to balance achieving justice against the public interest. Nonetheless, the court has to determine which material should not be disclosed, as made clear by Part 1 of the Criminal Procedure and Investigations Act 1996 and s.21(2) thus retains the common law approach which assesses whether the public interest applies in the circumstances. Part 22 of the Criminal Procedure Rules 2011 spells out the procedure which has to be followed by the prosecution when immunity is being sought.[488] The procedure requires that the other side is notified of the type of excluded material, but when this discloses too much or when even the disclosure that there is any other material is too sensitive then an *ex parte* application can also be made.[489] However, a judge cannot reach a decision on the basis of evidence, which has been excluded on the basis of public immunity, as this would violate Article 6(1) of the ECHR, as made clear in *Edwards v UK*.[490] The issue is that s.15(3) of RIPA requires that intercept material is normally destroyed as soon as possible and may therefore not be seen by the judge. Keane and McKeown (2012) thus state that the scope for

[485] *Edwards and Lewis v United Kingdom* (2005) 40 EHRR 24, 53; cited from I. Walden, S. Ramage, Computer Crimes and Digital Investigations, Publication Review, 72(1) *Journal of Criminal Law* 2008, 87-88, 88
[486] *R v Governor of Brixon Prison, ex parte Osman* [1992] 1 All ER 108; A. Keane, P. McKeown, *The Modern Law of Evidence* (9th edn, Oxford, Oxford University Press 2012) 564
[487] [1992] 3 All ER 440
[488] A. Keane, P. McKeown, *The Modern Law of Evidence* (9th edn, Oxford, Oxford University Press 2012) 565
[489] Also see *R v Davis* [1993] 1 WLR 613, see especially Lord Taylor CJ; A. Keane, P. McKeown, *The Modern Law of Evidence* (9th edn, Oxford, Oxford University Press 2012) 565-566
[490] [2003] 15 BHRC 189

immunity on public policy grounds is very wide.[491] Choo (2012) points out that it is, for instance, available when national security, international comity or diplomatic relations requires this.[492]

Durston (2011) notes that in the House of Lords case of *Conway v Rimmer*,[493] it was made clear that the test balanced the administration of justice against non-disclosure for service to the state.[494] Lord Reid opined "*I do not doubt that there are certain classes of documents which ought not to be disclosed whatever their contents may be."*[495] He explained that *"[t]he police are carrying on an unending war with criminals many of whom are today highly intelligent. So it is essential that there should be no disclosure of anything which might give any useful information to those who organise criminal activities."*[496]

Yet in *Burmah Oil Co Ltd v Bank of England,*[497] Lord Keith disagreed when he noted "*The courts are....concerned with the consideration that it is in the public interest that justice should be done and should be publicly recognized as having been done. This may demand,...in a very limited number of cases, that the inner workings of government should be exposed to public gaze, and there may be some who would regard this as likely to lead, not to captious or ill-informed criticism, but to criticism calculated to*

[491] A. Keane, P. McKeown, *The Modern Law of Evidence* (9th edn, Oxford University Press 2012) 568
[492] A. L.-T. Choo, *Evidence* (3rd edn, Oxford, Oxford University Press 2012) 205
[493] [1968] AC 910
[494] G. Durston, *Evidence, Text & Materials* (2nd edn, Oxford, Oxford University Press 2011) 554
[495] *Conway v Rimmer* [1968] AC 910, 952
[496] *Conway v Rimmer* [1968] AC 910, 953-4
[497] [1980] AC 1090

improve the nature of that working as affecting the individual citizen."[498] However, this was not a criminal case, but concerned a claim by an oil company against the Bank England which had entered into an agreement to be rescued in accordance with the UK's economic policy and the disclosure request related to sensitive government documents. However, Munday (2013) explains that the exclusion of police sources is generally affirmed; so long as the defendant does not depend on the information to prove his innocence.[499]

In certain circumstances it may also be necessary to conduct *"closed material procedures"* and special advocates have to be instructed, as highlighted by the Supreme Court case of *Al Rawi v Security Service*.[500] In this case, two cases were conjoined to address the issue whether the government can litigate matters by employing closed procedures and secret evidence.[501] The Al Rawi case concerned civil claims for mistreatment, rendition and detention against the UK government, whereas the Tariq case was an employment tribunal case against the Home Office. It was held that parliament has to adopt legislation in order to permit that civil claims can be conducted by way of *"closed material procedures."*[502]

---

[498] *Burmah Oil Co Ltd v Bank of England* [1980] AC 1090, 1134; also see *Air Canada v Secretary of State for Trade (No.2)* [1983] 2 AC 394, 432 per Lord Fraser

[499] Also see *Marks v Beyfus* [1890] 25 QBD 494, 498, per Lord Esher MR; R. Munday, *Evidence* (7th edn, Oxford, Oxford University Press 2013) 126

[500] [2011] UKSC 34; A. Keane, P. McKeown, *The Modern Law of Evidence* (9th edn, Oxford University Press 2012) 591

[501] M. Ryder, Case Preview: Al-Rawi v Security Service, Tariq v Home Office, UK Supreme Court Blog, 2 March 2012 <http://ukscblog.com/case-preview-al-rawi-v-security-service-tariq-v-home-office/> accessed 15th August 2015

[502] A. Gearey, W. Morrison, R. Jago, *The Politics of the Common Law: Perspectives, Rights, Processes, Institutions* (2nd ed, Abingdon, Routledge 2013) 267

Furthermore, pursuant to s.17 of RIPA, communications content is inadmissible; the section states that:

> *"(1) ... no evidence shall be adduced, question asked, assertion or disclosure made or other thing done in, for the purposes of or in connection with any legal proceedings which (in any manner) -*
>
> *(a) discloses, in circumstances from which its origin in anything falling within subsection (2) may be inferred, any of the contents of an intercepted communication or any related communications data; or*
>
> *(b) tends (apart from any such disclosure) to suggest that anything falling within subsection (2) has or may have occurred or be going to occur."*

This section is a re-enactment of s.9 of Interception of Communications Act 1985, RIPA's predecessor.[503] Hence, revealing that an authorisation has been granted to intercept remains proscribed.[504] Gersch (2012) points out that the problem with this section is that advocates are barred from submitting on behalf of their clients that they have been under surveillance, even if this is the case.[505]

The UAE should also adopt legislation, which regulates instances in which evidence does not need to be disclosed, particularly in light of its plans to heavily invest in surveillance technology.

---

[503] Editorial, Admissibility; Criminal evidence; Privacy; Surveillance; Telecommunications, *Criminal Law Review* 2000, 877-878, 877
[504] C. Tapper, *Cross & Tapper on Evidence* (12th edn, Oxford, Oxford University Press 2010) 522
[505] A. Gersch, Covert surveillance - a snoopers' charter? *Archbold Review* 2012, 5-8, 6

1.15 Summary

The literature review has set out the theoretical context and relevant social science literature on cybercrime in relation to the legislative framework adopted by the UK, EU and UAE. Key cybercrime terms have been defined and some of the challenges which have to be overcome in order to successfully fight cybercrime have been highlighted. As cybercrime is an emerging phenomenon, this constitutes a new field of study and which constantly raises new questions. For instance, the classification of cybercrime may change in the future in line with rapid technological innovation, which offers cyber criminals new criminal opportunities. Whilst previous research exists, this research is important, as it contributes to the ongoing debate of how to successfully fight cybercrime which is a dynamic and volatile phenomenon requiring new, innovative and effective legislative and policy responses.

The cybercrime laws, which the UK has adopted, have been analysed and problems have been identified, as well as how these have been addressed. The UK has a wide arsenal of statutes, which can be evoked to prosecute cyber criminals and this caters for the ubiquitous nature of cybercrime. These laws have also been updated in light of European initiatives to fight cybercrime. The brief history of combating cybercrime at the European level has been studied and the latest steps, which have been taken, have been discussed. The European approach relies on mutual assistance in respect of criminal matters, establishing contact points for high-tech crime and setting up specialised agencies to fight cybercrime. A twin strategy is run through the creation of

ENISA, which is entrusted with protecting information systems. Legislative steps have also been taken in respect of attacks against information systems, particular offences have been created on a European wide basis and further measures have been adopted to harmonise rules in respect of jurisdiction, cooperation and liability. A European cyber security strategy has also been adopted, which places particular emphasis on safeguarding network and information security, including through reporting requirements.

Subsequently, the literature review has critically discussed the cybercrime laws, which the UAE has adopted. It has been observed that Federal Legal Decree No. 5 for 2012 on combating cybercrimes is an important step to promote privacy, though other steps should also be taken in order to reinforce data security, which is a crucial constituent of any successful cybercrime strategy, as highlighted by the European approach.

The surveillance laws in the UK have been studied, as without these law enforcement officers cannot effectively police the digital realm, which is characterised by anonymity. These laws are particularly instructive for the UAE, which at present has not put surveillance powers on a sufficient statutory footing, as also discussed in this literature review. Yet it is also important to avoid some of the criticism, which has been levied against the UK and the European approach, especially following the recent CJEU decision in *Google Spain SL v Agencia Espanola de Proteccion de Datos (AEPD),*[506] which highlights the importance to adopt effective safeguards against abuse, to safeguard data privacy and proportionality when data is being retained and used for

[506] (C-131/12) (2014) 164(7607) NLJ 20

law enforcement purposes. The Google case has brought to the fore two kinds of criticism: Firstly that it was wrong to extend the term "data controllers" to search engine operators; and secondly, that the decision favours data erasure and thus overprotects the right to privacy and thereby empowers individuals too much and permits censorship without a proper oversight mechanism at the expense of the right to freedom of information or expression.[507] The case could have been avoided if Data Protection Directive 95/46/EC had been clear on that point or if the proposed General Data Protection Regulation had already been adopted. The UAE should therefore improve its legislative framework for privacy and data protection in line not only with the old Data Protection Directive, but the European reform proposals, which are specifically designed to foster a digital market, which can cope with cyber attacks and are viewed as part of a twin strategy against cybercrime.

The literature review also analysed the UK evidence rules on admissibility for criminal proceedings and the relevant rules governing circumstances of public policy non-disclosure. These are very important, as data retention and data surveillance serve to facilitate law enforcement. Accordingly, a legislative framework has to be adopted by the UAE to spell out in which circumstances evidence is considered admissible or inadmissible. After having reviewed the applicable literature, the next Chapter will explain the methodology which will be used to meet the research objective to comprehensively compare the legislative frameworks, which the UK, the European Union and the UAE have adopted to combat e-crime in order to develop

[507] Google Spain SL v. Agencia Española de Protección de Datos, 128 Harvard Law Review 2014, 735 <http://harvardlawreview.org/2014/12/google-spain-sl-v-agencia-espanola-de-proteccion-de-datos/> accessed 10th August 2015

recommendations, which will strengthen the existing legislative e-crime landscape and result in cybercrime being more effectively combated in the UAE.

Chapter Two: Methodology

2. Introduction

Fundamentally, the research seeks to realise the research objectives and for this reason a mixed method approach was chosen. This approach combined methods from law and the social sciences. The researcher is a pragmatist and tried to find a practical solution to the problem of cybercrime and considered that reality is not just objective, but also subjective. It was therefore considered that methodological pluralism enriches the research, since the different research methods permit triangulation, as originally developed by Denzin.[508] Accordingly, a number of methods were used to investigate the research question and to increase the validity and reliability of the findings.[509]

The methodology followed the legal positivist tradition which assumes that knowledge can be ascertained from objective facts, i.e. laws[510] and also drew upon the interpretivist approach in using qualitative interviewing. As the legislative response to cybercrime is mainly driven by external factors, as well as the social and political context of the development of legislation, and this is a new and emerging legal area, social science methods were also employed.[511] This approach was selected to explore the impact and

[508] N. K. Denzin, *The Research Act in Sociology* (Chicago, Aldine 1970) 50
[509] J. Kuada, *Research Methodology: A Project Guide for University Students* (Frederiksberg, Samfundslitteratur 2012) 61
[510] W. E. Conklin, *The Invisible Origins of Legal Positivism: A Re-Reading of a Tradition* (Kluwer Academic Publishers 2001) 9
[511] M. McConville, W. Hong Chui, *Research Methods for Law* (Edinburgh University Press 2007) 3

effectiveness of existing e-crime legislation and to address the research question.[512] This is also known as *"the third wave"* or *"third paradigm"*, which was combined with the philosophical companion of pragmatism in order to guide the design framework for the mixed methods research.[513] Consequently, the research was considered through the paradigm or lens of positivism and also interprevitism. As the research is particularly law-driven, the research may also be perceived as a type of postpositivism, because it implicitly supports the type of truth finding and analysis linked to positivism.[514] A postpositivist conceptualisation of law perceives law realistically and understands it as falling within the sphere of social reality, and as existing outside the realm of legal scholarship, despite this also resulting in co-creation within a pragmatically evolving legal system.[515]

In terms of the structure, this chapter starts with an explanation of the researcher's ontological and epistemological world view. It is explained how this view influenced the research philosophy, design and strategy. Thereafter, the research methods are discussed, namely the doctrinal legal analysis/black letter law approach, the comparative method and empirical research. Subsequently, the chapter examines sensitive and ethical issues, the qualitative interviewing technique, and the type of sampling which was employed. The setting of the interviews and method of recording are described, as well

[512] S. N. Hesse-Biber, *Mixed Methods Research, Merging Theory with Practice* (New York, The Guildford Press 2010) 215
[513] R. B. Johnson, Mixed Methods Research: A Research Paradigm Whose Time Has Come, 33(7) *Educational Researcher* 2004, 14-26, 14; D. Ary, L. Cheser Jacobs, C. Sorensen, A. Razvieh, *Introduction to Research in Education* (8th edn, Belmont, Wadsworth Cengage Learning) 559
[514] L. S. Giddings, B. M. Grant, A Trojan Horse for Positivism?: A Critique of Mixed Methods Research, 30(1) *Advances in Nursing Science* 2007, 52-60, 52
[515] A. Grabowski, *Juristic Concept of the Validity of Statutory Law: A Critique of Contemporary Legal Nonpositivism* (Berlin, Springer 2013) 539

as how data quality was achieved. Data analysis techniques are discussed and how the researcher maintained ethics and ensured that the qualitative research can be published.

2.1 Ontology

The term *"ontology"* denotes the philosophical base for a particular theory and is the foundational underpinning of the theory.[516] Guba and Lincoln observe that *"paradigm issues are crucial; no inquirer, we maintain, ought to go about the business of inquiry without being clear about just what paradigm informs and guides his or her approach."*[517] As the research adopts a mixed methods approach, it is underpinned by a combination of positivism and interpretivism, though the black letter approach may not be perceived as truly positivist in the social science sense as it is a form of documentary analysis which is categorised as a qualitative approach in social research.[518]Despite criticisms that these two systems of inference (positivism and interpretivism) are irreconcilable polarities, it has been convincingly argued that using both can enrich and even fine-tune research findings. On this matter it has been asserted that whereas positivists identify and recognise patterns in qualitative data, an interpretivist will try to establish why the patterns exist, by looking for the causal mechanisms at work and the context in which they occur, when applied together it is believed they are very effective tools in generating and implementing sustainable solutions based on the research findings, which is in accord with the ultimate aims of this study. [519]

---

[516] D. Hartas, *Educational Research and Inquiry: Qualitative and Quantitative Approaches* (London, Continuum International Publishing Group 2010) 15
[517] E. G. Guba, Y. S. Lincoln, Competing paradigms in qualitative research in (eds) N. K. Denzin, Y. S. Lincoln, *Handbook of Qualitative Research* (Thousand Oaks, SAGE 1994) 105-117, 116
[518] S. M. Redpath, R. J. Gutiérrez, A. Evely, K. A. Wood, J. C. Young, *Conflicts in Conservation* (Cambridge, Cambridge University Press 2015) 110
[519] A C Lin, Bridging Positivist and Interpretivist Approaches to Qualitative Methods, (26) 1 *Policy Studies Journal* 1998, 162-180

Essentially, it may be more accurate to perceive these two paradigms as being rooted within *"communities of practice"*, as different methods were mixed, this may better lend itself to the pragmatist origins, for it integrates the inherent diversity and results in the various methodological selections being better understood.[520] This means that the research is more practice-based, there is more collaboration connected to the core research objective and increased flexibility and permeability, moreover, there is no monolithic way, but an amalgamation of various research entities.[521] Accordingly, the researcher considers that an overly restrictive labelling of numerical data into quantitative and other methods as qualitative could frustrate the underlying objective of the mixed method approach, which is not necessarily concerned with creating separateness between positivism and interpretivism.[522] In this context, it is emphasised that this research is predominantly concerned with legal positivism, which is different to typical positivism with its overwhelming emphasis on a numerical approach. Nonetheless, even without falling into the trap of perceiving mixed method research as a disjointed amalgamation of two opposing paradigms, it is crucial to consider each paradigm in turn, as well as its philosophical roots.

---

[520] M. Denscombe, Communities of practice: a research paradigm for the Mixed Methods approach, De Montford University, 2008, 1-26, 1

[521] Ibid, 14-15

[522] J. E. Symonds, S. Gorard, The Death of Mixed Methods: Research Labels and their Casualties, The British Educational Research Association, Annual Conference, Heriot Watt University, Edinburgh, 3-6 September 2008, 1-19, 1 <http://www.leeds.ac.uk/educol/documents/174130.pdf> accessed 20th July 2015

In terms of the ontology, positivism assumes that there is a stable and objective reality, and that laws and legal cases and the development of the law can be observed and measured. It is therefore assumed that reality is distinct from the experience of a person, irrespective of the beliefs of a person.[523] Reality is therefore external since objects, subjects and responsibilities, as well as values and rules objectively exist and can be identified.[524] Positivism is characterised by its logical, rational and verbal approach, which is free of value judgements.[525] Similarly, legal positivism perceives law as value-free principles which can be identified since they have been "posited", generally through rules which have been enacted through the proper legislative process.[526] Knowledge is therefore created from scientific, legal, scholarly methods in line with the realist ontology, as laws and cases can be objectively identified.[527]

Positivism originates in France and assumed importance after the French Revolution. It was promulgated by Claude-Henri de Saint-Simon and Auguste Comte, who sought to introduce an element of natural science into the study of society.[528] For Comte, positivism perceives all research phenomena to be governed by natural laws and emphasises the importance of discoverable facts over unobservable causes. The positivist movement was also influenced by Weber and Durkheim, who further paved

[523] B. Hjorland, Empiricism, rationalism and positivism in library and information science, 61(1) *Journal of Documentation* 2005, 130-155, 140
[524] R. Sharman, R. Kishore, R. Ramesh, *Ontologies: A Handbook of Principles, Concepts and Applications in Information Systems* (New York, Springer Science & Business Media LLC 2007) 160
[525] D. Carson, S. Gilmore, C. Perry, K Gronhaug, *Qualitative Marketing Research* (London, SAGE Publications Inc 2005) 5
[526] R. M. Cotterrell, *Émile Durkheim: Law in a Moral Domain* (Stanford, Stanford University Press 1999) 216; L. Blaxter, C. Hughes, M. Tight, *How to Research* (4th edn, Maidenhead, Open University Press 2010) 61
[527] M. Denscombe, *Ground Rules for Social Research, Guidelines for Good Practice* (2nd edn, Maidenhead, McGraw-Hill Education 2010) 119
[528] G. Snooks, *The Laws of History* (Abingdon, Routledge 1998) 91

the way for a more scientific approach towards sociology.[529] Weber employed causality to bridge the gap between social science and natural science.[530] Durkheim looked at the given and viewed it as part of the natural order and thus as a manifestation and focused on discovering this given, thereby embracing an inherently realist view towards the theory of knowledge.[531] He embraced a form of "idealist empiricism;" he looked for "social facts" which were created through a collective conscience made up of external limitations and norms, and that were internalised by people through their socialisation and moral and cultural education.[532]

Parsons built upon Durkheim's sociology and perceived it as a move away from "radical positivism" to "analytical realism."[533] For Parsons, positivism is a methodological tool i.e. a means to depict complicated opinions about the criteria and drivers which funnel action and society.[534] Parsons viewed everything being objectively observed as positive facts and which can therefore be counted as reality and constituted as "total thought."[535] Both Durkheim and Parsons were concerned with the issue of order through a "functionalist conception of social systems." [536]

---

[529] A. Giddens, Classical Social Theory and the Origins of Modern Sociology, 81(4) *American Journal of Sociology* 1976, 703-729, 703
[530] D. F. Lindenfeld, *The Transformation of Positivism: Alexius Meinong and European Thought, 1880-1920* (Los Angeles, University of California Press 1980) 176
[531] P. Q. Hirst, *Durkheim, Bernard and Epistemology* (Abingdon, Routledge 2011) 4
[532] C. Casey, *Critical Analysis of Organizations: Theory, Practice, Revitalization* (London, SAGE Publications Ltd 2002) 49
[533] T. Parsons, The Structure of Social Action (London, McGraw Hill 1937) 708-714; B. C. Wearne, *The Theory and Scholarship of Talcott Parsons to 1951: A Critical Commentary* (Cambridge, Cambridge University Press 2009) 68
[534] H. P. M. Adriaansens, *Talcott Parsons and the Conceptual Dilemma* (Abingdon, Routledge 2015) 34
[535] Ibid, 35
[536] C. Casey, *Critical Analysis of Organizations: Theory, Practice, Revitalization* (London, SAGE Publications Ltd 2002) 49

For Parsons, social equilibrium is established through "four functional imperatives". First, there has to be "adaptation" so that acts are adapted to link the environment to the system; second, there has to be "goal attainment", this requires acts which lead to resources being made available to realise and achieve these goals; third, there has to be "integration", so that these acts are controlled and coordinated; and fourth, there has to be "pattern maintenance"/"latency", so that those who perform these acts are sufficiently motivated.[537] Hence, the way in which relations are being structured between people engaged in cooperative processes is "essentially the structure of the social system."[538] A common value system is thereby created which promotes social integration since society shares the same norms, standards and expectations.[539] With respect to this study, the legal system is a "social system"[540] which is made up of legally valid rules which the legislators and courts have authoritatively stipulated.[541] However, this system predominantly centres on legal relationships, as opposed to legal rules, though legal norms facilitate increased understanding of these relationships.[542]

Durkheim and Parsons are often associated as the forefathers of functionalist theory which underpins positivism.[543] Functionalism has four distinct features: Firstly, functionalism emphasises that human conduct has fixed characteristics and structures,

[537] J. Hassard, *Sociology and Organization Theory: Positivism, Paradigms and Postmodernity* (Oxford, Oxford University Press 1995) 22
[538] H. Ross, *Law as a Social Institution* (Portland, Hart Publishing 2001) 163
[539] J. Hassard, *Sociology and Organization Theory: Positivism, Paradigms and Postmodernity* (Oxford, Oxford University Press 1995) 22
[540] H. Ross, *Law as a Social Institution* (Portland, Hart Publishing 2001) 163
[541] R. Siltala, *A Theory of Precedent: From Analytical Positivism to a Post-analytical Positivism to a Post-analytical Philosophy of Law* (Oxford, Hart Publishing 2000) 43
[542] H. Ross, *Law as a Social Institution* (Portland, Hart Publishing 2001) 163
[543] P. W. Cookson, A. R. Sadovnik, 'Functionalist Theories of Education' in (eds) D. Levinson, P. Cookson, A. Sadovnik, *Education and Sociology: An Encyclopedia* (Abingdon, Routledge 2001) 267

and these macrostructures are what is being studied; secondly, it is assumed that social structures can preserve or weaken social structure and it is therefore investigated how these structures fulfil their function; thirdly, functionalists argue that these structures depend on common values; and fourthly, functionalism has been perceived as a force to create stability and impose conservative values.[544] A key preoccupation of functionalism is *"equilibrium,"* since the functional approach is closely associated with promulgating a *"theory of society as a whole or totality"*, whilst perceiving *"society as an integrated social system."*[545] Under this structural theory, as first espoused by Merton, individual behaviour is the result of social structures.[546] By way of an example, Chapman uses cultural standards and norms which produce *"value consensus."*[547] Hence, it is assumed that social arrangements contribute greatly to creating and maintaining society.[548]

Merton is another advocate of functionalism, though of a more flexible form, which incorporates empirical applications.[549] He advocates functional equivalence and argues that institutions can have negative and positive effects on society or specific groups, and recommends linking empirical findings with theory as utilised in this study.[550] He criticises Parsons for making absolute statements and was of the opinion that theorising by itself is insufficient, but that empirical studies are required to depict "empirical social

[544] R. Brym, J. Lie, *Sociology: Your Compass for a New World* (2nd ed, Belmont, Wadsworth Cengage 2010) 9
[545] R. A. Morrow, C. A. Torres, *Social Theory and Education: A Critique of Theories of Social and Cultural Reproduction* (Albany, State University of New York 1995) 41-42
[546] R. K. Merton, *Social Theory and Social Structure* (New York, The Free Press 1948)
[547] S. Chapman, *Sociology* (London, Letts and Lonsdale 2004) 24
[548] G. Ritzer, J. M. Ryan, *The Concise Encyclopedia of Sociology* (Chichester, John Wiley & Sons 2011) 239
[549] Ibid
[550] Ibid

reality."[551] This type of functionalism is a useful perspective for empiricism and positivism.[552] This is because positive studies are based on an ontology of a nomothetic methodology, which examines big groups to identify general norms of behaviour which apply to all.[553] "Nomos" is Greek and means "laws"[554] and considers that persons are a complex amalgamation of a variety of universal rules, so it is better to observe a large group.[555] The quantitative methodology lends itself towards identifying such laws since the person becomes subsumed within what others say through statistical means.[556] Deterministic laws can thereby be identified through mechanical natural science methods.[557] However, the application of such laws may be unethical and the findings may only generate superficial accounts.[558]

Moreover, the manner in which laws are interpreted or enforced can vary from case to case, and this is another reason why the paradigm of interpretivism has also been chosen for the research, as the researcher believes that reality is a social construct.[559] As persons create social reality, interpretivism emphasises "understanding"[560] i.e. interpreting what meaning individuals give and assign to a particular phenomenon.[561] Hence, reality is

---

[551] J. Hughes, W. Sharrock, *Theory and Methods in Sociology: An Introduction to Sociological Thinking and Practice* (Basingstoke, Palgrave Macmillan 2007) 7
[552] J. Heil, *Philosophy of Mind: A Contemporary Introduction* (London, Routledge 2002) 88
[553] E. Babbie, *The Practice of Social Research* (14th ed, Boston, Cengage Learning 2016) 93
[554] A. Stevenson, *Oxford Dictionary of English* (Oxford, Oxford University Press 2010) 1206
[555] R. L. Michalski, T. K. Shackelford, 'Evolutionary Perspectives on Personality Psychology' in (eds) G. J. Boyle, G. Matthews, D. H. Saklofsk, *The SAGE Handbook of Personality Theory and Assessment, Vol.2 Personality Measurement and Testing* (London, SAGE 2008) 167
[556] Ibid
[557] A. Gelman, J. Cortina, *A Quantitative Tour of the Social Sciences* (Cambridge, Cambridge University Press 2009) 60
[558] T. Abbott, *Social and Personality Development* (Hove, Routledge 2001) 11
[559] B. C. Stahl, *Information Systems, Critical perspectives* (Abingdon, Routledge 2008) 57
[560] P. M. Kasi, *Research: What, Why and How?: a Treatise from Researchers to Researchers* (Bloomington, Author House 2009) 96
[561] N. Blaikie, *Designing Social Research* (2nd edn, Cambridge, Polity Press 2009) 99

made up of these "interpretative processes" and the researcher therefore reconstructed the accounts by those who were interviewed into a scientific description about the research topic.[562] This interpretive approach is rooted in a relativist epistemology, an ideographic methodology, nominalism and a voluntary perspective of human identity.[563]

Epistemic relativism opposes the perspective that statements can be objectively assessed or universally applied since general views are not permanent. Rather, they can be determined by the population being influenced to hold such a belief, or could be the result of intellectual efforts to realise unity of interests.[564] It thus introduces relativism, scepticism and subjectivism.[565] As a relativist, absolute knowledge does not exist because it can be observed that opinions about different subjects vary and the assumptions on which these views are based depend on the background or the particular circumstances which the person has experienced.[566] Accordingly, such a stance considers that facts are not absolute facts and epistemic relativism contends that the knowledge which persons hold can change and is relative and that therefore all knowledge is relative and it is only possible to identify the facts which a person holds at a time, but that there are no absolute standards which justify these assumptions.[567]

---

[562] D. Scott, M. Morrison, *Key Ideas in Educational Research* (London, Continuum International Publishing Group 2006) 131
[563] D. J. Falconer, D. R. Mackay, The Key to the Mixed Method Dilemma, Proclamation of 10th Australasian Conference on Information Systems 1999, 286-297, 288 <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.5.148&rep=rep1&type=pdf> accessed 1st August 2015
[564] S. Luper, Epistemic Relativism, 14 *Philosophical Issues Epistemology* 2004, 271-295, 271
[565] Ibid
[566] M. Seidel, *Epistemic Relativism: A Constructive Critique* (Basingstole, Palgrave Macillan 2014) 9
[567] J. Matheson, 'Epistemic Relativism' in (eds) A. Cullison, *The Bloomsbury Companion to Epistemology* (London, Bloomsbury 2014) Chapter 9

Idiographic research focuses on examining individuals in order to obtain unique knowledge about them which is very detailed.[568] The word "idios" means "own" or personal" in Greek and when such an approach is adopted humans are perceived as inimitable.[569] The qualitative approach is particularly useful to comprehensively understand the person since it is more flexible and exhaustive since knowledge is created which is situational and contextual which allows that broad themes and categories can be developed.[570] Individual opinions about the research phenomenon become comprehensively understood, including particular issues which would otherwise not have been identified.[571] However, the issue is that idiographic studies are unscientific and do not generate results which can be generalised due to the unrepresentative sample and subjective processes.[572] As a result, it is often argued that such research studies cannot address real-world issues, despite the fact that these studies are conducted in a natural setting, which is less controlled than quantitative studies.[573]

Interpretive research is also influenced by an ontological perspective based on nominalism.[574] Nominalism holds that individuals are the "building blocks" which

[568] E. Babbie, *The Practice of Social Research* (14th ed, Boston, Cengage Learning 2016) 93
[569] I. Fairholm, *Issues, Debates and Approaches in Psychology* (Basingstoke, Palgrave Macmillan 2012) 20
[570] M. Saini, A. Shlonsky, *Systematic Synthesis of Qualitative Research* (Oxford, Oxford University Press 2012) 65
[571] Ibid
[572] M. Sandelowski, J. Barroso, *Handbook for Synthesizing Qualitative Research* (New York, Springer Publishing Company Inc 2007) 2
[573] Ibid
[574] D. J. Falconer, D. R. Mackay, The Key to the Mixed Method Dilemma, Proclamation of 10th Australasian Conference on Information Systes 1999, 286-297, 288 <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.5.148&rep=rep1&type=pdf> accessed 1st August 2015

underlie "constructivistic systems."[575] Individual parts make up reality, which renders it difficult to recognise universalism, since primacy is afforded to the specific.[576] Nominalism finds its underpinnings in extensionalism[577] which does not accept characteristics, attributes or properties of classes since they are aggregates and do not permit the individual to be identified.[578] For nominalists, words are only used meaningfully to identify whether a statement is false or true, but not to identify universally true statements since words are syncategorematic i.e. are not generally universals.[579] A nominalistic approach therefore supposes that everything is individualistic and it is therefore not the task to look for the general in the specific and as a result themes of knowledge do not give rise to a separate reality, though modern nominalists compare "individuals and sums of their parts."[580] Modern nominalism focuses on the individual or individual characteristics and reduces the metaphysical reality to actual existence and thereby rejects abstract ideas and universals and engages in a dialect between what is going on outside and inside the mind since concepts are subjective and personal since terms are determined by the meaning which a person assigns to it and truth is thus established through communicating unique data, particular perceptions and representations.[581] This form of epistemology is driven by autonomy and individualism and depends on what can be inferred through consciousness and what

[575] M. Gosselin, *Nominalism and Contemporary Nominalism: Ontological and Epistemological Implications of the work of W.V.O. Quine and of N. Goodman* (Dordrecht, Kluwer Academic Publishers 1990) 1
[576] Ibid, 2
[577] Ibid, 4
[578] W. Van Orman Quine, D. Føllesdal, D. B. Quin, *Confessions of a Confirmed Extensionalist: And Other Essays* (Harvard, Harvard University Press 2008) 11
[579] Ibid, 14
[580] M. Gosselin, *Nominalism and Contemporary Nominalism: Ontological and Epistemological Implications of the work of W.V.O. Quine and of N. Goodman* (Dordrecht, Kluwer Academic Publishers 1990) 96-97
[581] M. W. Oleksy, *Realism and Individualism: Charles S. Peirce and the Threat of Modern Nominalism* (Amsterdam, John Benjamins Publishing Co 2015) 81

thoughts are formed because of signs and theories, so that real knowledge can only come from obvious certitudes through a first person perspective because the human mind creates knowledge and objective recognition from what there is or builds it therefrom through logic based on what is purposeful, practical and ontic.[582] This also presupposes that individuals volunteer data.[583]

These different philosophical bases underlying the paradigm of positivism and interpretivism guided the researcher. The question of *"what there is"*[584] was thus not just answered from the objective, but also the subjective stance, resulting in a more in-depth understanding of the research phenomenon.[585] The researcher therefore assumed that the world exists, i.e. adopted a realist position, whilst he also considered that the human mind creates the world, i.e. a constructionist position was employed.[586]

2.2 Epistemology

The term *"epistemology"* denotes the particular paradigm or worldview and very often has been described as *"theories of knowledge"* or *"ways of knowing"* or more precisely *"the individual lens, created through our world view that we use to understand*

[582] Ibid, 81-82
[583] Ibid
[584] Stanford Encyclopedia of Philosophy, Logic and Ontology, 2011 <http://plato.stanford.edu/entries/logic-ontology/#DifConOnt> accessed 18 June 2014
[585] R. W. Belk, *Handbook of Qualitative Research Methods in Marketing* (Cheltenham, Edward Elgar Publishing Ltd 2006) 198
[586] M. Denscombe, *Ground Rules for Social Research, Guidelines for Good Practice* (2nd edn, Maidenhead, McGraw-Hill Education 2010) 119

knowledge in the world."[587] In terms of the epistemology for this research, it is primarily considered that the reality is objective and *"beyond the human mind"* and this is why the main chosen method for this doctrinal research was a *"content analysis."*[588] This thus constitutes expository research since laws and cases, which represent black letter law, were studied.[589] Empiricism was thus endorsed, i.e. objectivism, as opposed to the interpretive approach, but due to the mixed method research approach the subjective and qualitative experiences of individuals were also studied in line with the ontological foundations, discussed above.[590] Whilst laws arguably take precedence, this is not entirely the case since laws are interpreted and enforced by individuals.

Furthermore, by also adopting the interpretive approach, it was avoided that an overtly descriptive account of the law was given,[591] which is uncritical.[592] Interprevitism looks at reality as being inherently subjective and therefore emphasise understanding, as opposed to offering causal explanations, which positivism does.[593] By opting for mixed methods research, the researcher chose the *"third wave"*, as no purist stance was taken i.e. the researcher did not solely pursue a positivist or interpretivist research method.[594]

---

[587] J. Egbert, S. Sanden, *Foundations of Education Research: Understanding Theoretical Components* (Abingdon, Routledge 2014) 16-17
[588] B. Hjorland, Empiricism, rationalism and positivism in library and information science, 61(1) *Journal of Documentation* 2005, 130-155, 140
[589] D. Watkins, M. Burton, *Research Methods in Law* (Routledge 2013) 16
[590] E. Pivcevic, *Husserl and Phenomenology* (Routledge 2014) 85; R. Bohnsack, N. Pfaff, W. Weller, *Qualitative Analysis and Documentary Method in International Educational Research* (Barbara Budrich Publishers 2010) 100
[591] N. MacCormick, O. Weinberger, *An Institutional Theory of Law: New Approaches to Legal Positivism* (Springer 1986) 229
[592] W. Twining, *General Jurisprudence, Understanding Law from a Global Perspective* (Cambridge University Press 2009) 517
[593] L. Blaxter, C. Hughes, M. Tight, *How to Research* (3rd edn, Maidenhead, Open University Press 2006) 60
[594] D. Ary, L. Jacobs, A. Razavieh, C. Sorensen, *Introduction to Research in Education* (8th edn, Belmont, Wadsworth Cengage Learning 2010) 559

Instead a pragmatic approach, which utilised the advantages of each method and minimised the disadvantages associated with each respective method, was chosen.[595]

2.3 Research Philosophy

The philosophy underlying the methodology helps in identifying the most suitable methods to evaluate the data and therefore assists with answering the research questions. Hence, the chosen philosophy should be explained, since this facilitates critical thinking and leads to the development of other questions.[596]

The philosophical assumptions underlying the mixed methods approach influenced the research methods and the nature of the inquiry since they represented the underlying worldviews on which the study was based.[597] Johnson and Gray explicate that *"[d]uring the emergence of [Mixed Methods (MM)] MM as a third methodological paradigm (along with [quantitative] QUAN and [qualitative] QUAL), MM has struggled somewhat with to develop a corresponding philosophical paradigm. Many or perhaps most leaders in the field are advocating some form of philosophical pragmatism."*[598]

A pragmatic research philosophy was chosen, so that *"theory and practice"* can be captured and not much emphasis was placed on *"intellectual disputes"* between

[595] Ibid
[596] Also see M. J. Smith, Social Science in Question London (London, Sage 1998)
[597] J. W. Creswell, V. L. P. Clark, *Designing and Conducting Mixed Methods Research* (2nd ed, London, SAGE Publications Ltd 2011) 38
[598] R. Johnson, R. Gray, 'A history of philosophical and theoretical issues for mixed methods research' in (eds) A. Tashakkori, C. Teddlie, *SAGE Handbook of Mixed Methods in Social & Behavioral Research* (California, SAGE 2010) 69-94, 87

positivism and interpretivism.[599] Hence, overall a pragmatic research philosophy was adopted, as the objective approach was mixed with the subjective stance.[600] This pragmatic stance did override adherence to one specific paradigm, but instead viewed the two worldviews as additional methodological and practical choices.[601] This necessitated familiarity with the arguments in favour and against mixed methods, required that risks were taken and choices were justified.[602] Yet one of the issues with pragmatism is that it may result in thoughtless practicalism and epistemic relativism, so that subjectivism becomes applied to logic and facts.[603] Resultantly, the researcher tried to robustly defend all choices and perspectives.

2.4 Research Choices

Positivism perceives that reality is objective and this suggests that the researcher should be detached from the research participants and employ techniques, which accord with the natural science approach.[604] Whilst positivism is normally associated with quantitative data collection methods and statistical analysis, it is important to point out that this is slightly different in relation to law.[605] The researcher did not use questionnaires to gather data. Nonetheless, this research scrutinised data from the

[599] P. Baert, F. C. da Silva, *Social Theory in the Twentieth Century and Beyond* (Cambridge, Polity Press 2010) 294&296
[600] Also see M. Y. Feilzer, Doing Mixed Methods Research Pragmatically: Implications for the Rediscovery of Pragmatism as a Research Paradigm, 4(1) *Journal of Mixed Methods Research* 2010, 1-16, 1
[601] R. Cameron, Mixed Methods Research: The Five Ps Framework, 9(2) *Electronic Journal of Business Research Methods* 2011, 96-108, 102 <http://ejbrm.com/volume9/issue2> accessed 1st August 2015
[602] P. Brazeley, Teaching mixed methods, 3 *Qualitative Research Journal* 2003, 117-126, 118
[603] R. Cameron, Mixed Methods Research: The Five Ps Framework, 9(2) *Electronic Journal of Business Research Methods* 2011, 96-108, 97 <http://ejbrm.com/volume9/issue2> accessed 1st August 2015
[604] L. Blaxter, C. Hughes, M. Tight, *How to Research* (3rd edn, Maidenhead, Open University Press 2006) 60
[605] Also see M. Van Hoecke, *Preference to Methodologies of Legal research, which kind of method for What Kind of Discipline?* (London, Hart Publishing 2011) Chapter 10

positivist perspective of thought.[606] This means that the quantitative parts of the thesis were explanation- and description-oriented and the literature played a fundamental role and provided the justification for conducting the research and the findings were clearly observable and specific and the data were the legal statutes and cases, which were analysed and interpreted and objective and unbiased conclusions were drawn.[607] The qualitative part of the research focused on understanding and was therefore more exploratory and the literature did not play an important role or did not provide justifications for the research.[608] Instead the opinions and experiences of a small group of individuals were centre-stage, so that the data was broad and general. Their descriptions were analysed and themes were developed in order to ascertain the bigger picture behind the findings and conclusions were drawn, but which were flexible and emergent and also possibly biased.[609]

2.5 Research Design, Approach and Strategy

As the research is predominantly rooted in legal positivism, inductive reasoning was primarily employed. Induction is the base of positivism, as made clear by the founding

[606] J. C. Alexander, *Positivism, Presuppositions, and Current Controversies* (Abingdon, Routledege 2014) 2
[607] Also see R. Cottrell, J. F. McKenzie, *Health Promotion & Education Research Methods: Using the Five Chapter Thesis/Dissertation Model* (2nd ed, London, Jones and Bartlett Publishers International 2011) 6
[608] C. Daymon, I. Holloway, *Qualitative Research Methods in Public Relations and Marketing Communications* (2nd ed, Abingdon, Routledge 2011) 47
[609] Also see R. Cottrell, J. F. McKenzie, *Health Promotion & Education Research Methods: Using the Five Chapter Thesis/Dissertation Model* (2nd ed, London, Jones and Bartlett Publishers International 2011) 6

fathers of legal positivism, starting with Bentham, Austin, Kant and later Kelsen and who separated law from morality, which thereby aided with the claim that law resembles more the empiricist paradigm.[610]

However, as a mixed method approach was pursued, deductive reasoning supplemented this main approach.[611] When deductive logic was employed, a true conclusion was reached when the evidence supported this.[612] In contrast, inductive logic implies a conclusion which is uncertain and exceeds the evidence.[613] Inductive reasoning is thus called "bottom up thinking" because it starts with specifics and moves to the abstract and general principles.[614] This approach is data-driven.[615] Instead deductive logic applies rules or general observations to guestimate specifics and this approach is therefore described as "top-down."[616] This approach is hypothesis-driven.[617] Deductive logic generates either invalid or valid conclusions, whereas inductive logic can be strong or weak and all depends on how much the conclusion is supported by the evidence.[618] An inductive approach was adopted for the black-letter law analysis and the comparative

[610] T. Campbell, *Prescriptive Legal Positivism: Law, Rights and Democracy* (London, UCL Press 2004) 29-30
[611] J. C. Greene, *Mixed Methods in Social Inquiry* (San Francisco, John Wiley & Sons Inc 2007) 77
[612] J. C. Dixon, R. Singleton, B. C. Straits, *The Process of Social Research* (Oxford, Oxford University Press 2016) 20
[613] Ibid
[614] E. DePoy, S. French Gilson, *The Human Experience: Description, Explanation, and Judgment* (Lanham, Rowman & Littelfield Publishing Group Inc 2007) 21
[615] E. Hung, *Philosophy of Science Complete: A Text on Traditional Problems and Schools of Thought* (2nd ed, Boston, Wadsworth Cengage Learning 2014) 267
[616] E. DePoy, S. French Gilson, *The Human Experience: Description, Explanation, and Judgment* (Lanham, Rowman & Littelfield Publishing Group Inc 2007) 21
[617] E. Hung, *Philosophy of Science Complete: A Text on Traditional Problems and Schools of Thought* (2nd ed, Boston, Wadsworth Cengage Learning 2014) 267
[618] J. C. Dixon, R. Singleton, B. C. Straits, *The Process of Social Research* (Oxford, Oxford University Press 2016) 20

legal research.[619] Accordingly, the researcher commenced "from the purpose of the study and move...on to delineate specific research questions."[620] Additionally, a qualitative analysis was conducted, as even a clear legislative regime can result in unreliable decisions and as this thesis combines a legal and social science methodological approach. Deductive reasoning was therefore employed to identify themes from the data provided by the interviewees.[621] Deductive logic was also used to apply the legal rules to factual situations i.e. to refer to examples provided by the interviewees and to draw conclusions.[622] Unique insights were thereby gained, for instance, about the specific actions of individuals.[623]

2.6 Doctrinal Legal Analysis

A doctrinal or black letter law approach was adopted for a significant part of the thesis, as the relevant laws in the UK, the European Union and the UAE were studied.[624] This form of research "provides a systematic exposition of the rules governing a particular legal category, analyses the relationship between rules, explains areas of difficulty and, perhaps, predicts future developments."[625] Accordingly, an in-depth legal analysis of

[619] D. E. McNabb, *Research Methods in Public Administration and Nonprofit Management, Quantitative and Qualitative Approaches* (New York, M. E. Sharpe Inc 2013) 9
[620] L. S. Connaway, R. R. Powell, *Basic Research Methods for Librarians* (Santa Barbara, Greenwood Publishing Group 2010) 211
[621] A. J. Hatch, *Doing Qualitative Research in Education Settings* (New York, State University of New York, 2002) 161
[622] A. Knight, L. Ruddock, *Advanced Research Methods in the Built Environment* (Chichester, Blackwell Publishing Ltd 2008) 32
[623] D. E. Gray, *Doing Research in the Real World* (3rd edn, London, Sage Publications Ltd 2014) 23
[624] M. McConville, W. Hong Chui, *Research Methods for Law* (Edinburgh University Press 2007) 3
[625] D. Pearce, E. Campbell, D Harding, Australian Law Schools: A Discipline Assessment for the Commonwealth Tertiary Education Commission (Sydney, Australian Government Publishing Service

cybercrime laws, data protection, data retention, data surveillance and digital evidence laws, and case law in the UAE and UK was carried out. Hence, all relevant primary sources, such as UK Acts of Parliament, European legislation and UAE laws and cases, were studied. Additionally, relevant secondary sources, such as books, journals, articles, reports, webpages, were examined to present important arguments and debates by academics. [626] The law was faithfully presented and this necessitated a "sound legal analysis" and the researcher viewed the doctrinal methodology as "a process...to achieve pragmatic solutions" after a careful review of the applicable literature, so that it became fully understood "what is known and not known."[627] The researcher first identified relevant sources and subsequently analysed and interpreted these in order to identify core ideas and to condense these by employing problem solving and reasoning skills, drawing analogies and making use of inductive and deductive reasoning.[628]

Furthermore, the research adopted a critical perspective when laws were analysed. Hence, not just a descriptive account was provided of the applicable legal rules, but the law was also put into context.[629] Otherwise, the research may have resulted in a *"narrow-minded black letter"* approach, which *"lack[s] the intellectual capacities to go beyond the mere technical analysis of positive law."*[630] For instance, it was explored whether any gaps exist within the legislative framework which the UAE has adopted, particularly when benchmarked against UK e-crime legislation and the European

1987) in (eds) T. Hutchinson, *Researching and Writing in Law* (3rd edn, London, Reuters Thomson 2010) 7

[626] Also see R. K. Yin, *Case Study Research: Design and Methods* (4th edn, Sage Publications 2009) 160

[627] D. Watkins, M. Burton, *Research Methods in Law* (Abingdon, Routledge 2013) 13

[628] Ibid

[629] F. Cownie, *Legal Academics: Culture and Identities* (Oxford, Hart Publishing 2004) 49-50

[630] M. Adams, J. Bomhoff, *Practice and Theory in Comparative Law* (Cambridge University Press 2012) 305

approach towards data retention and network and information security. Equally, this is not just a highly conservative study, which precludes a discussion of law reform, as issues are highlighted.[631] For instance, the European Commission recently highlighted why the UK Data Protection Act 1998 appears to fall foul of EU Directive 95/46/EC and such criticism is discussed and born in mind when recommendations were formulated for the UAE.[632]

2.7 Comparative Legal Research

The comparative method was adopted, and knowledge was gathered about the UK and European Union approaches and then the UAE framework was studied to identify differences and similarities.[633] This method was chosen to suggest legislative solutions for the global problem of cybercrime and to generate new knowledge. Laws were compared and a new perspective to the currently adopted regime in the UAE was described.[634] This was useful because an understanding was reached about the UAE's legal system. The research therefore helps in grasping the UAE's view on this important topic. It allows the UAE to borrow ideas in this newly emerging field, whilst taking into account the UAE's particular legal, economic and social culture.[635]

---

[631] T. Campbell, *Prescriptive Legal Positivism: Law, Rights and Democracy* (Routledge-Cavendish 2004) 329

[632] Amberhawk, 2011 <http://amberhawk.typepad.com/amberhawk/2011/02/european-commission-explains-why-uks-data-protection-act-is-deficient.html> accessed 3 May 2014

[633] P. G. Monateri, *Methods of Comparative Law* (Edward Elgar Publishing Ltd 2012) 151

[634] Also see J. Church, C. Schulze, H. Strydom, *Human Rights from a Comparative and International Law* (University of South Africa 2007) 7

[635] Also see H. Gutteridge, *Comparative law; an introduction to the comparative method of legal study and research* (2nd edn, Wildy 1974) 70

There are various reasons for choosing the UK and the EU as a comparator: The UK approach is different to the e-crime legislation, which the UAE has adopted. As developed countries with a strong technological base, the UK and EU have a well-developed digital space, which has aided online business and e-commerce.[636] The comparative approach thus served to generate "model solutions", as the UK and European framework offer "a greater variety of solutions than could be thought up in a lifetime by even the most imaginative jurist who was corralled in his own system."[637] A very comprehensive understanding was reached about the underlying legal principles in an area of law that requires legal reform in most countries around the world.[638] By explaining how the UK, EU and the UAE currently regulate this area, it also becomes easier for governments to co-operate, as the legal rules and principles are being communicated.[639] New insights were also gained when the English common law system and European system were studied and compared to the UAE system, which is based on the religious Sharia law, as different families of law were analysed.[640]

2.8 Empirical Legal Research

The empirical method was chosen in order to assess the impact of the law. This is important as cybercrime laws are utilised and enforced by law enforcement agencies and

[636] J. Reuvid, *The Secure Online Business Handbook: A Practical Guide to Risk Management and Business Continuity* (4th edn, London, Kogan Page Ltd 2006) 21
[637] K. Zweiaert, H. Koetz, *An Introduction to Comparative Law* (Oxford University Ores 1998); cited from M. Gu, *Understanding Chinese Company Law* (2nd edn, Hong Kong University Press 2010) 5
[638] Also see D. Watkins, M. Burton, *Research Methods in Law* (Routledge 2013) 16
[639] L. Blaxter, C. Hughes, M. Tight, *How to Research* (3rd edn, Maidenhead, Open University Press 2006) 315
[640] J. M. Smits, *Elgar Encyclopedia of Comparative Law* (Edward Elgar Publishing Inc 2006) 390

interpreted by judges and relied upon by other stakeholders, such as businesses. Not that many cybercrime cases have been heard in the UAE and conducting interviews helped to understand the experiences of relevant stakeholders involved in combating cybercrime or affected by it. The researcher therefore interviewed a small sample of senior UAE experts from the judiciary, police, the office of prosecution, Interpol and the Telecommunications Regulatory Authority. A qualitative interview approach was employed in order to enable a full exploration of the topic.

This method ensured that the UAE law was put into context, as social, economic and political factors were considered, including the different interests of stakeholders, namely government and enforcement agencies. Hence, the research took into account economic, social, political factors, as *"[l]aw is...the vernacular through which power and wealth justify their exercise and shroud their authority."*[641] The views of these very high-ranking individuals assumed much importance.[642]

2.9 Researching Sensitive Issues and Ethics

[641] Also see Q. A. Acton, *Issues in Law Research* (Scholarly Editions 2013) 94

[642] B. Hjorland, Empiricism, rationalism and positivism in library and information science, 61(1) *Journal of Documentation* 2005, 130-155, 130; D. Valenzuela, P. Shrivastava, Interview as a Method for Qualitative Research, 1-20, 1 <http://www.public.asu.edu/~kroel/www500/Interview%20Fri.pdf> accessed 3 May 2014; also for details about qualitative interviews, see A. A. Trainor, E. Graue, *Reviewing Qualitative Research in the Social Sciences* (Routledge 2013) 132

The researcher took due account that research may deal with sensitive matters i.e. matters which are stressful or private, lead to fear or branding or are politically laden.[643] For instance, research about child abuse has been found to cause distress to participants who were themselves victims.[644] Equally a topic is sensitive when a threat arises as a result of the data collection or the data dissemination may cause problems for the researcher. [645] The type of individuals who are being interviewed may also be affected.[646] In this context, Lee explicates that there can be three kinds of threats: firstly, those which are intrusive, secondly, those which have a sanction and thirdly, those which have political ramifications. [647] As a result, the researcher may be stigmatised due to the research topic, his career may be affected, for instance, because matters have been revealed which should not have been disclosed, the researcher may receive anonymous threats or face presentational dangers because of the publication being associated with the researcher. [648] Hence, a very comprehensive approach was adopted and it was therefore considered whether there is indirect harm and not just typical subject matters were classified as sensitive topics.

Research highlights that sometimes researchers have to cope with emotionally or physically difficult issues and that it is therefore important that researchers are

[643] H. McCosker, A. Barnard, R. Gerber, Undertaking Sensitive Research: Issues and Strategies for Meeting the Safety Needs of All Participants, 2(1) *Forum Qualitative Social Research* 2001 <http://www.qualitative-research.net/index.php/fqs/article/view/983/2142> accessed 15 July 2015
[644] S. E. Decker, A. E. Naugle, R. Carter-Visscher , K. Bell, A. Seifert, Ethical Issues in Research on Sensitive Topics: Participants' Experiences of Distress and Benefit, 6(3) *Journal of Empirical Research on Human Research Ethics: An International Journal* 2011, 55-64, 55
[645] Ibid
[646] V. Dickson-Swift, E. L. James, P. Liamputtong, *Undertaking Sensitive Research in the Health and Social Sciences, Managing Boundaries, Emotions and Risks* (Cambridge, Cambridge University Press 2008) 1
[647] R. M. Lee, *Doing Research on Sensitive Topics* (London, SAGE 1993) 4
[648] Ibid; G. Adshead, C. Brown, *Ethical Issues in Forensic Mental Health Research* (London, Kessica Kingsley Publishers Ltd 2003) 91

sufficiently trained, prepared and there is supervision, in order to ensure that any risks are mitigated.[649] Consequently, possible problems have to be anticipated and the researcher has to be prepared to end a research relationship in a courteous manner when this appears necessary.[650] The personal safety of the researcher is also ensured by not furnishing personal address and contact details, conducting the interviews in public locations and alerting another person of the interview location and meeting time or adopting a lone working policy, using a SIM card for a phone number which is solely used for the research, carefully observing whether the interviews trigger any emotional responses and having regular debriefings with a supervisor.[651] However, this research was not sensitive or emotionally or physically challenging.

Most fundamentally, the researcher acknowledges that he owes a duty of care.[652] This duty of care is owed to multiple parties, for instance, colleagues, research subjects and the research community.[653] Ethical behaviour commands adherence to various fundamental values: Firstly, scrupulous honesty, so that research findings are not fabricated or fraudulent; secondly, integrity, so that the research is rooted on firm moral principles and consistent beliefs and values; thirdly; fairness, so that benefits and burdens resulting from the research are equally shared; and fourthly, respect, so that all those who are involved in the research are duly venerated, including by upholding their

[649] V. Dickson-Swift, E. L. James, S. Kippen, P. Liamputtong, Risk to Researchers in Qualitative Research on Sensitive Topics: Issues and Strategies, 18(1) *Health Policy & Services* 2008, 133-144, 133
[650] D. Fahie, Doing Sensitive Research Sensitively: Ethical and Methodological Issues in Researching Workplace Bullying, 13(1) *International Journal of Qualitative Methods* 2014, 19-36, 19
[651] Ibid, 29
[652] Ibid
[653] M. Petre, *The Unwritten Rules of PhD Research* (2nd ed, Maidenhead, Open University Press 2010) 1-7

rights.[654] Moreover, compliance with the principles of justice, beneficence and autonomy can be used to overcome tensions between the research objectives and the rights of the interview participants.[655]

Additionally, research participants were shielded from any harm and whilst the research topic does not deal with controversial matters, it was ensured that interviews were in no way distressing.[656] The researcher obtained written consent from the Ministry of Justice in the UAE to conduct this research.[657] Furthermore, informed consent was sought from the research participants and 'informed' not only meant that those who participated in the research appreciated that they authorised the researcher, but also in respect of which aspects and the latter required details about the objectives of the research, the methods, risks, discomforts and inconveniences and how the findings will be used, for instance, for the publication of articles or the thesis.[658] This necessitated that research participants were provided with sufficient information to understand to what they consented to, but it may not always be easy to determine what a person considers material to reach their decision to participate.[659]

The participants were informed that they can refuse to take part and are only volunteers, who can even throughout the entire process refuse their consent to participate.[660] The

[654] C. Standing, *How to Complete a PhD* (Craig Standing 2012) 134
[655] A. Orb, L. Eisenhauer, D. Wynaden, Ethics in Qualitative Research, 33(1) *Journal of Nursing Scholarship* 2001, 93-96, 93
[656] A. Faulkner, *The Ethics of Survivor Research: Guidelines for the Ethical Conduct of research carried out by mental health service users and survivors* (Bristol, The Policy Press 2004) 8
[657] C. Russell, L. Hogan, M. Junker-Kenny, *Ethics for Graduate Researchers, A Cross-Disciplinary Approach* (London, Elsevier Inc 2013) 132
[658] M. Israel, I. Hay, *Research Ethics for Social Scientists* (London, SAGE Publications Ltd 2006) 61
[659] Ibid, 62
[660] I. Holloway, L. Brown, *Essentials of a Qualitative Doctorate* (Walnut Creek, Left Coast Press Inc 2012) 195

research participants were not coerced, persuaded or manipulated to reach a particular decision.[661] This ensured that primacy was given to the research participants and their autonomy was not being evaded.[662]

As the thesis also contains qualitative findings, which are detailed and rich and describe unique circumstances, there was a higher danger that confidentiality may be compromised.[663] The researcher therefore ensured that anonymity was preserved. The names of those who participate were kept anonymous.[664] Before data was collected, interviews were assigned letters, for instance, each interview participant had a specific letter assigned (i.e. interviewee A) and the name of the persons was noted down on a separate sheet, which is kept in a different and secure location (i.e. in a locked filing cabinet or password protected electronic device) which only the researcher can access.[665]

Moreover, information about the characteristics of participants which may identify them, such as occupation or city, was not disclosed, so that no deductive disclosure takes place and internal confidentiality is maintained.[666] The main objective was to

[661] M. Israel, I. Hay, *Research Ethics for Social Scientists* (London, SAGE Publications Ltd 2006) 62
[662] M. Israel, I. Hay, *Research Ethics for Social Scientists* (London, SAGE Publications Ltd 2006) 60
[663] K. Kaiser, Protecting Respondent Confidentiality in Qualitative Research, 19(11) *Qualitative Health Research* 2009, 1632-1641, 1632
[664] P. Cryer, *The Research Student's Guide to Success* (3rd edn, Maidenhead, Open University Press 2006) p.87
[665] N. King, C. Horrocks, *Interviews in Qualitative Research* (London, SAGE Publications 2010) 118
[666] M. Tolich, Internal confidentiality: When confidentiality assurances fail relational informants, 27 *Qualitative Sociology* 2004, 101–106, 101; J. Sieber, Planning ethically responsible research: A guide for students and internal review boards (Newbury Park Sage 1992) 52

achieve full confidentiality for each research participant.[667] A thorough data cleansing process was followed and rare traits which may identify individuals were deleted, but the issue is that there may still remain contextual identifiers.[668] In such instances, data was modified in a way which did not alter essential information.[669] In cases where it was not possible to remove personal identifiers, consent was sought from the particular interview participants to nonetheless release the data.[670]

Moreover, 'off the record' comments were not included, as this would breach confidentiality, though the researcher clarified whether and if so, in which way the research participants felt comfortable to have such information included in the research.[671] After conclusion of each interview, debriefings took place, so that feedback could be provided, research participants were thanked for their participation and provided with interview transcripts and details about how to obtain possible results from the research.[672] Participants were also enabled to access any personal content and to read interview transcripts and to point out inaccuracies and comment on the content.[673] They could also choose that their comments were not included.[674]

---

[667] B. Baez, Confidentiality in qualitative research: Reflections on secrets, power and agency, 2 *Qualitative Research* 2002, 35–58, 32
[668] M. Tolich, Internal confidentiality: When confidentiality assurances fail relational informants, 27 *Qualitative Sociology* 2004, 101–106, 102
[669] K. Kaiser, Protecting Respondent Confidentiality in Qualitative Research, 19(11) *Qualitative Health Research* 2009, 1632-1641, 1634
[670] Ibid
[671] R. Wiles, *What are Qualitative Research Ethics?* (London, Bloomsbury Academic 2013) 50
[672] E. A. Buchanan, *Readings in Virtual Research Ethics: Issues and Controversies* (London, Information Science Publishing 2004) 19
[673] S. E. Israel, C. A. Lassonde, *The Ethical Educator, Integrating Ethics within the Context of Teaching and Teacher Research* (New York, Peter Lang Publishing Inc 2007) 23
[674] Also see D. C. Blankenship, *Applied Research and Evaluation Methods in Recreation* (Leeds, Human Kinetics 2010) 78

Not only the common law duty of confidentiality was guaranteed, but there was full compliance with the Data Protection Act 1988, including the following eight data protection principles:[675] Personal information was fairly and lawfully processed; the processing only took place in respect of limited purposes; the processing was relevant, adequate and not disproportionate; accuracy was maintained; data was not retained for a longer period than what was necessary; the processing was undertaken in compliance with the rights of the data subjects; the data was kept secure; and data protection was also adequate in case it was transferred to a country outside the European Economic Area (EEA).[676]

As the data was retained for some time, the data was properly managed and kept securely.[677]

Strategies were adopted to ensure secure storage, for instance, back-ups were made, data was stored in open standard and non-proprietary formats, data was stored on different types of storage; paper notes were stored in PDF and a secure location was used to keep the data which can only be accessed by the researcher; confidential data was not stored on external networks; regular security updates were made and the computer was protected by a firewall; passwords were used to lock the computer system and encryption was employed to control access; and confidential data was not be sent by email, but only as encrypted file.[678] Data will not be stored for more than five years and

---

[675] T. Long, M. Johnson, *Research Ethics in the Real World: Issues and Solutions for Health and Social Care* (Philadelphia, Elsevier Ltd 2007) 75

[676] Schedule 1 of the Data Protection Act 1998

[677] Prof. C. Standing, *How to Complete a PhD* (Craig Standing 2012) 136

[678] V. van den Eynden, L Corti, M. Woolard, L. Bishop, L. Horton, Managing and Sharing Data, 3rd ed, UK Data Archive, May 2011, 1-40, 18-19 <http://www.data-archive.ac.uk/media/2894/managingsharing.pdf> accessed 1st August 2015

will thereafter be destroyed.[679] Paper-based documents will be shredded in accordance with the German Institute for Standardisation DIN 3 standard, which requires confetti like bits no bigger than 4x40 mm or strips no bigger than two millimetre.[680] Digital files will be overwritten several times until they are permanently deleted and additionally, a magnet may be used to erase the data.[681]

Throughout the research, it was ensured that the research was conducted in accordance with the University's ethical code of conduct and the highest ethical standards.[682]Ethics permission has been gained from the university's ethics committee and the research adheres to the British Society of Criminology's Code of Ethics for Researchers in the Field of Criminology.[683]

2.10 Qualitative Interviewing

The researcher conducted interviews and this method provided a more in-depth understanding of the topic than if quantitative methods were used for instance,

[679] N. King, C. Horrocks, *Interviews in Qualitative Research* (London, SAGE Publications 2010) 118
[680] V. van den Eynden, L Corti, M. Woolard, L. Bishop, L. Horton, Managing and Sharing Data, 3rd ed, UK Data Archive, May 2011, 1-40, 20 <http://www.data-archive.ac.uk/media/2894/managingsharing.pdf> accessed 1st August 2015
[681] T. Long, M. Johnson, *Research Ethics in the Real World: Issues and Solutions for Health and Social Care* (Philadephia, Elsevier Ltd 2007) 79
[682] M. Petre, G. Rugg, *The Unwritten Rules of PhD Research* (2nd edn, Maidenhead, Open University Press 2010) 107; also see British Society of Criminology, Code of Ethics for Researchers in the Field of Criminology, undated, 1-6 <http://www.britsoccrim.org/docs/CodeofEthics.pdf> accessed 1 February 2015
[683] British Society of Criminology's Code of Ethics for Researchers in the Field of Criminology, undated, 1-6 <http://www.britsoccrim.org/docs/CodeofEthics.pdf> accessed 1st December 2015

surveys.[684] Semi-structured interviews were held i.e. core questions were developed in order to outline the topics which were discussed, thereby permitting the interviewee or interviewer to deviate during the interview, so that more data could be provided about particular matters.[685] Hence, this type of interview was more flexible than structured interviews and made it possible that participants could speak about matters which they considered important in relation to the research topic.[686] Yet the disadvantage was that it was more difficult to interpret follow-up questions since not all participants answered the same follow-up question and this may result in bias, for instance, if the interviewer only probed particular questions or did this in a particular manner.[687]

The objective of conducting interviews was to ascertain the beliefs, experiences and views about the legal cybercrime framework and to explore the way in which the framework operates in practice. As the cybercrime legal regime is fairly new and this is an emerging topic, not much is known about the impact of UAE cybercrime laws which have been enacted. Open-ended questions were asked which generated a lot of data about the research phenomenon and which aimed to answer the research objectives.[688] The researcher also enquired about the background and occupation of the interview participant, so that these could be located in respect to other persons.[689]

---

[684] I. R. Williams, *Strategic Planning in Small Businesses: A phenomenological study investigating the role, challenges, and best practices of strategic planning* (Minnesota, ProQuest 2008)
[685] N. Britten, Qualitative interviews in healthcare in (eds) C. Pope N. Mays, *Qualitative research in health care* (2nd ed, London, BMJ Books 1999) 11
[686] P. Gill, K. Stewart, E. Treasure, B. Chadwick, Methods of data collection in qualitative research: interviews and focus groups, 204 *British Dental Journal* 2008, 291-295 < http://www.nature.com/bdj/journal/v204/n6/full/bdj.2008.192.html> accessed 4th August 2015
[687] M. Mitchell, J. Jolley, *Research Design Explained* (7th ed, Belmont, Wadsworth 2010) 277
[688] M. Q. Patton, *Qualitative Research & Evaluation Methods: Integrating Theory and Practice* (4th ed, London, SAGE Publications Ltd 2015) 446
[689] Ibid, 445

The researcher did not ask leading, double-barrelled or long questions, or questions which negated or had a socially desirable answer or influenced subsequent questions and care was taken when questions were worded and plain and simple langue was used to avoid that participants misinterpret the question and irrelevant matters were not probed.[690] Questions dealing with easy and noncontroversial topics were asked first, followed by questions which required participants to express their opinion and skill and knowledge questions were only asked subsequently to prevent that the participants felt threatened.[691] The researcher also provided the participants the questions in advance, so that they could familiarise themselves with the topics before the interviews.

2.11 Sampling

Sampling denotes purposefully selecting an aspect of the entire population in order to generate insight and this raises the question who should be chosen and how this selection should be made. [692] The quantitative probability sampling method is inappropriate for qualitative research since it contravenes the qualitative concept of appropriateness which necessitates a purposive sample.[693] As the researcher conducted qualitative research, the researcher therefore employed non-probability purposive

[690] M. Mitchell, J. Jolley, *Research Design Explained* (7th ed, Belmont, Wadsworth 2010) 303-304
[691] M. Q. Patton, *Qualitative Research & Evaluation Methods: Integrating Theory and Practice* (4th ed, London, SAGE Publications Ltd 2015) 445-446
[692] I. Holloway, S. Wheeler, *Qualitative Research in Nursing and Healthcare* (3rd ed, Chichester, John Wiley & Sons 2010) 137
[693] M. N. Marshall, Sampling for qualitative research, 13(6) *Family Practice* 1996, 522-526, 522

sampling, so that data was generated which is relevant and information-rich.[694] The purposive non-random sample consisted of the top five people in the UAE, namely an officer at the Department of Cybercrime in the UAE, who was seconded to Interpol for the period from 2012 to 2016; the Chief and Head of the Public, Civil and Commercial Department at Fujairah Court, who was previously the Head of the Department of Information Technology at the Fujairah Federal Court of First Instance; the Head of Department of Electronic Investigations at the General Directorate of Investigations at Dubai Police; the Chief at Dubai Public Prosecution and the Legal Advisor/Counsel for the Telecommunications Regulatory Authority. Hence, the most senior experts in the field were interviewed. These experts shared their knowledge, which has formed the foundation of the research. The characteristics of the individuals were used as the basis of selection and reflected the diversity and breadth of the sample population.

The characteristics and features of these senior UAE experts were known to the researcher. The persons were deliberately chosen because they were the main experts in the field in the UAE. The most senior cybercrime judge was interviewed, as he not only knew the relevant laws, but was also aware of practical legal issues which hindered successful prosecutions. Similarly, the researcher interviewed one of the most experienced police officers specialised in electronic investigations. The officer was not only familiar with the relevant laws, but was acutely aware which problems existed in respect of procedural. evidential and other matters. The public prosecutor was interviewed who deals with most cybercrime cases because he not only knew the law, but could identify what undermine the effectiveness of combating cybercrime in the

[694] R. K. Yin, *Qualitative Research from Start to Finish* (2nd ed, New York, The Guilford Press 2016) 93

UAE. An officer who had worked for Interpol was interviewed in light of his experience, especially in the field of international cooperation. Cybercrime can often only be successfully investigated through cooperation with other countries and this interview particularly elucidated issues in relation to this, but also other common legal problems. In the UAE, the Telecommunications Regulatory Authority is at the forefront of preventing cyber attacks.[695] For this reason, a senior officer was interviewed who knew the legal framework of the UAE.

It was not particularly difficult for the researcher to identify these experts, as he knew who was particularly familiar with the research topic. He therefore chose the main cybercrime experts since they were most likely to be knowledgeable and articulate.[696] Hence, the researcher chose interview participants based on the objectives of the research and the role which they performed within organisations was a starting point.[697] This approach is also called criterion sampling since participants were selected on the basis of fixed criteria.[698] By applying predetermined criteria, quality was assured.[699] Opting for a purposive non-random sample was called for to stay within the framework and within the field of interest and also because the researcher had only a limited

[695] WAM, Telecommunications Regulatory Authority prevents 289 cyber-attacks in Q1 2017, Emirates247, 31 July 2017 <http://www.emirates247.com/news/emirates/telecommunications-regulatory-authority-prevents-289-cyber-attacks-in-q1-2017-2017-07-31-1.656939> accessed 1st December 2017
[696] I. Holloway, S. Wheeler, *Qualitative Research in Nursing and Healthcare* (3rd ed, Chichester, John Wiley & Sons 2010)
[697] I. T. Coyne, Samplying in qualitative research. Purposeful and theoretical sampling; merging or clear boundaries? 26 *Journal of Advanced Nursing* 1997, 623-630, 624
[698] W. A. Pitney, J. Parker, *Qualitative Research in Physical Activity and the Health Professions* (Windsor, Human Kinetics 2009) 42
[699] M. Q. Patton, *Qualitative Research & Evaluation Methods: Integrating Theory and Practice* (4th ed, London, SAGE Publications Ltd 2015) 281

amount of time.[700] Consequently, the sample was not meant to be a statistically representative sample.[701]

Moreover, the number of people interviewed was less important than the criteria used to select them. Nonetheless, it is acknowledged that a sample which is small offends the quantitative idea which holds that there has to be a sufficient sample size to render findings representative.[702] A too small sample may not realise theoretical saturation or informational redundancy, whilst a too large sample may not allow a thick and detailed analysis which is the underlying purpose of qualitative research.[703] The sample selection had thus a bearing on the overall quality of the work.[704] As it was unknown how many individuals had to be interviewed for the data collection process, interviews were continued until data saturation was reached and no new information was being generated from the interview process.[705]

It must be stressed that as a judge, the researcher had unprecedented access. It would not have been possible to access these people if not for the researcher's senior judicial position. Also, as an insider, the researcher not only shared the same culture and language. He also worked in the legal industry and thus had similar characteristics as

---

[700] L. Schatzman, A. L. Strauss, *Field Research Strategies for a Natural Sociology* (Englewood Cliffs, Prentice Hall 1973) 39
[701] J. Ritchie, J. Lewis, C. McNaughton Nicholls, R. Ormston, *Qualitative Research Practice: A Guide for Social Science Students and Researchers* (2nd ed, London, SAGE Publications 2013) 113
[702] J. M. Morse, Strategies for sampling in (eds) J. M. Morse, *Qualitative Nursing Research: A Contemporary Dialogue* (Newsbury Park, SAGE 1991) 127
[703] M. Sandelowski, Sample size in qualitative research, 18(2) *Research in Nursing & Health* 1995, 179-183, 179
[704] I. T. Coyne, Sampling in qualitative research. Purposeful and theoretical sampling; merging or clear boundaries? 26 *Journal of Advanced Nursing* 1997, 623-630, 623
[705] H. Brink, C. Van der Walt, G. Van Rensburg, *Fundamentals of Research Methodology for Health Care Professionals* (2nd ed, Cape Town, Juta & Co (Pty) Ltd 2006) 134

those interviewed. The researcher's experience and position meant that the researcher felt as belonging to those who were interviewed.[706] The researcher was knowledgeable and could easily interact with the experts.[707] Equally, the interviewees felt that the researcher belonged to the same social group i.e. had similar characteristics.[708] As a result, they felt comfortable sharing their views with the researcher. This arguably makes the work even more unique and rigorous. However, it is also acknowledged that being an inside researcher also poses the risk of being subjective and biased.[709] Such criticism was addressed since the researcher approached the research phenomenon from a wide legal perspective which was not limited by the UAE legal approach. He was also not afraid to pose questions which challenged the current legal status quo in the UAE.

The researcher also intended to interview UK experts. He therefore contacted the Crown Prosecution Service in order to arrange an interview with a UK prosecutor, as well as the National Cybercrime Unit and the Metropolitan Police Cybercrime Unit. He also contacted Lockheed Martin and BAE Systems, as well as some other UK companies. However, regrettably all declined to take part in the interviews (please see 'Example of an Interview Request to a UK Expert' and 'Response Received to an Interview Request from a UK Expert' in the Appendices).. The reason why those contacted declined to take part in interviews are unknown. Although it highlights that having unprecedented access

[706] L. Kirpitchenko, L. Voloder, *Insider Research on Migration and Mobility: International Perspectives on Researcher Positioning* (Farnham, Ashgate Publishing Ltd 2014) 87; M. J. Greene, On the Inside Looking In: Methodological Insights and Challenges in Conducting Qualitative Insider Research, *The Qualitative Report* 19(29), 1-13, 2
[707] Ibid (Greene) 3-4
[708] N. A. Anples, *Feminism and method: Ethnography, discourse analysis, and activist research* (New York, Routledge 2003) 46.
[709] M. Crossley, L. Arthur, E. McNess, *Revisiting Insider-Outsider Research in Comparative and International Education* (Oxford, Symposium Books Ltd 2015) 162

to senior UAE experts due to the researcher being a judge was a real advantage.

2.12 Conducting the Interviews and Recording the Data

An interview consists of a *"two-way conversation"* which should be interactive and dynamic.[710] For this to take place, the interview was opened with a short introduction which outlined the aims of the research, the importance of the information and key ethical issues, such as confidentiality and informed consent and this served as an *"icebreaker"*.[711] The questions were developed in advance, real questions were asked, the informants were provided with sufficient time to answer questions without being interrupted, the researcher engaged in active listening, so that the informants felt that they could answer without being judged and upon conclusion the researcher expressed gratitude for the time and information which the informant provided.[712]

The five face-to-face interviews took place in a private setting, for instance, in a private and quiet room at the offices of the research participants.[713] As the researcher worked alone and this poses certain risks, it was ensured that necessary precautions were taken, for instance, meeting details, including name and contact address and meeting location, were left with another person in case there was an emergency, thereby safeguarding the

[710] J. A. Hatch, *Doing Qualitative Research in Education Settings* (Albany, State University of New York Press 2002) 114
[711] Ibid
[712] J. A. Hatch, *Doing Qualitative Research in Education Settings* (Albany, State University of New York Press 2002) 114
[713] R. Edwards, J. Holland, *What is Qualitative Interviewing?* (London, Bloomsbury Academic 2013) 43

researcher's safety.[714] However, such risk was very low. The interviews were immediately translated from Arabic into English by the researcher and transcribed after each interview.[715] Interviewees were asked to sign a consent form.

2.13 Data Quality

Quality is a crucial objective of any research and this can only be attained if great care is taken throughout the different stages, starting with the research questions and continuing with the data collection, the data analysis and subsequent interpretation of the findings in light of the literature.[716] The researcher was guided by the meta-theory when developing the research questions and did not base the questions on *a priori* assumptions, for instance, which reflect the experience of the researcher or are the findings from similar studies, but instead the criterion was relevance alone.[717] During the data collection process, professionalism and ethics were maintained at all times; respondents were motivated, a good rapport and trust was developed;; there was active listening; what was being communicated was fully understood, including nonverbal cues; it was determined whether a response was sufficient and relevant and if not the researcher probed for responses; notes were prepared diligently; and data security was maintained at all times; and after each interview it was verified that the interview

[714] L. M. Given, *The SAGE Encyclopedia of Qualitative Research Methods* (London, SAGE Publications Ltd 2008) 778
[715] J. A. Hatch, *Doing Qualitative Research in Education Settings* (Albany, State University of New York Press 2002) 116
[716] M. M. Bergman, A. P. M. Coxon, The Quality in Qualitative Methods, 6(2) *Qualitative Social Research* 2005, 34 <http://www.qualitative-research.net/index.php/fqs/article/view/457/974#g21> accessed 15th July 2015
[717] Ibid

transcript is accurate and it was promptly imported into NViva.[718] More generally speaking, it was ensured that the research questions were consistent with the epistemology, the research objectives, the audience, methods, ethics and research recommendations.[719]

The adoption of these kinds of measures was important to render quality concerns an integral aspect in order to demonstrate accountability and validity.[720] Furthermore, by explicitly depicting what steps have been taken, another researcher would be able to determine how plausible the findings are.[721] Scientific rigour was thus demonstrated as described above, but the quantitative concepts of validity and reliability and generalisability were not perceived as useful for qualitative research.[722] Yet it is acknowledged that this is debated and some consider that some form of validity and reliability are important in qualitative research.[723] Nonetheless, these concepts rather belong to the toolkit of positivists.[724] This is because for qualitative researchers, there exists no *"objective social reality"*, but instead social reality is being constructed by individuals and there are therefore many different social realities which all have their

[718] G. Guest, K. M. MacQueen, *Handbook for Team-based Qualitative Research* (Lanham, Altamira Press 2008) 242-243
[719] A. E. Fortune, W. J. Reid, R. L. Miller, *Qualitative Research in Social Work* (2nd ed, Columbia, Columbia University Press 2013) 94
[720] M. M. Bergman, A. P. M. Coxon, The Quality in Qualitative Methods, 6(2) *Qualitative Social Research* 2005, 34 <http://www.qualitative-research.net/index.php/fqs/article/view/457/974#g21> accessed 15th July 2015
[721] Ibid
[722] E. Quimby*, Doing Qualitative Community Research: Lessons for Faculty, Students and Communities* (Danvers, Bentham Science Publishers 2012) 14-15; A. M. Clarvarion, J. M. Najman, D. Silverman, The Quality of Qualitative Data: Two Strategies for Analyzing Medical Interviews, 1(2) *Qualitative Inquiry* 1995, 223-242, 223
[723] D. Silverman, *Doing Qualitative Research: A Practical Handbook* (4th ed, London, SAGE Publications Ltd 2013) 301
[724] G. Winter, A comparative discussion of the notion of validity in qualitative and quantitative research, 4(3-4) *The Qualitative Report* 2000 <http://www.nova.edu/ssss/QR/QR4-3/winter.html> accessed 16th July 2015

distinct internal logic.[725] It can therefore not be determined which one has more validity than others.[726] This does not mean that the truthfulness of the data should not be ascertained, though Silverman concedes that for qualitative researchers this is an ambiguous objective.[727]

Equally, the concept of reliability within qualitative research is problematic since it affords "consistency or constancy of a measuring instrument."[728] This necessitates neutral, standardised and non-biased means to generate data.[729] However, human conduct is not constant or static and a repeated study will not yield the same outcome because for qualitative researchers no single and uniform reality exists.[730] It is therefore extremely difficult to fully standardise qualitative tools, also because interpretivists try and capture the background and context and not just narrow variables.[731]

Something akin to reliability within qualitative research is stability and this can be achieved by posing the same questions and having consistent answers and testing whether the same answers are received when equivalent questions are being asked.[732] It therefore appears more accurate to speak of "dependability" in respect of qualitative

[725] I. Holloway, *Qualitative Research in Health Care* (Maidenhead, Open University Press 2005) 13
[726] Ibid
[727] D. Silverman, *Interpreting qualitative data: Methods for analysing talk, text and interaction* (2nd ed, London, Sage Publications 2001) 5; D. Kalekin-Fishman, Review: David Silverman (2001). 'Interpreting qualitative data: Methods for analysing talk, text and interaction' (2001) 2(3) *Forum Qualitative Social Research*, 1, 3
[728] G. LoBiondo-Wood, J. Haber, *Nursing Research: Methods, Critical Appraisal and Utilisation* (2nd ed, St Louis, Mosby 1998) 558
[729] J. Mason, *Qualitative Researching* (London, SAGE 1996) 145
[730] S. B. Merriam, E. J. Tisdell, *Qualitative Research: A Guide to Design and Implementation* (San Francisco, John Wiley & Sons 2016) 250
[731] T. Long, M. Johnson, Rigour, reliability and validity in qualitative research, 4 *Clinical Effectiveness in Nursing* 2000, 30-37, 30
[732] P. Brink, Issues of reliability and validity in (eds) J. Morse, *Qualitative nursing research: a contemporary dialogue* (London, SAGE 1991) 176

research, as opposed to reliability.[733] Dependability denotes research procedures which are adequate and clear and this is realised by thoroughly documenting all research processes and decisions, for instance, by having memos which address possible questions about the research process.[734] The researcher therefore strived to document all processes in order to enable other researchers to replicate the research.[735] Just like reliability, the core concern of dependability is therefore that a consistent data collection process is followed, so that the data is not affected.[736]

Another important idea within qualitative research is internal consistency which requires that social reality is captured in an authentic manner.[737] The various voices and perspectives were articulated and any recommendations did not merely advocate "one size fits all...recommendations" which fail to take into account the different voices.[738] The criterion of credibility or believability therefore became a substitute for internal validity in respect of the qualitative research segment.[739] The way in which experiences, interpretations and internal knowledge was described was accurate and matched what

[733] T. Long, M. Johnson, Rigour, reliability and validity in qualitative research, 4 *Clinical Effectiveness in Nursing* 2000, 30-37, 31
[734] W. A. Pitney, J. Parker, *Qualitative Research in Physical Activity and the Health Professions* (Leeds, Human Kinetics 2009) 68
[735] A. K. Shenton, Strategies for ensuring trustworthiness in qualitative research projects, 22 *Education for Information* 2004, 63-75, 63
[736] T. Long, M. Johnson, Rigour, reliability and validity in qualitative research, 4 *Clinical Effectiveness in Nursing* 2000, 30-37, 31
[737] I. Holloway, *Qualitative Research in Health Care* (Maidenhead, Open University Press 2005) 13
[738] A. E. Fortune, W. J. Reid, R. L. Miller, *Qualitative Research in Social Work* (2nd ed, Columbia, Columbia University Press 2013) 94
[739] P. Leavy, *The Oxford Handbook of Qualitative Research* (Oxford, Oxford University Press 2014) 110

the participants reported.[740] Raw data in the form of quotes from participants was provided to enhance verisimilitude.[741]

This is not to say that the findings constitute objective facts or can be generalised since the concept of generalisability belongs to the positivist paradigm.[742] Generalisability can be understood as the extent to which conclusions from the research sample apply to the entire class or research phenomenon which is being studied.[743] Another description for generalisability is external validity or transferability.[744] Whilst qualitative work does not allow statistical generalisability, it generates in-depth descriptions and these permit to a certain degree flexible generalisability i.e. certain central themes may be captured which generate broad, thick and rich knowledge.[745]

Trustworthiness was enhanced through the adoption of the following strategies: Personal prejudice was accounted for in order to avoid that the findings became influenced, for instance, by critically scrutinising whether the sampling process was biased and the data collection process and analysis resulted in relevant data; by keeping accurate records, including a trail of all decisions, so that it is apparent why data was interpreted in a

[740] A. E. Fortune, W. J. Reid, R. L. Miller, *Qualitative Research in Social Work* (2nd ed, New York Columbia University Press 2013) 21
[741] Ibid
[742] M. Myers, Qualitative Research and the Generalizability Question: Standing Firm with Proteus, 4(3-4) The Qualitative Report 2000 <http://www.nova.edu/ssss/QR/QR4-3/myers.html> accessed 29th July 2015
[743] D. Polit, B. Hungler, *Nursing research: Principles and methods* (New York, JB Lippincott 1991) 645
[744] M. T. Blanche, K. Durrheim, D. Painter, *Research in Practice: Applied Methods for the Social Sciences* (2nd ed, Cape Town, University of Cape Town Press (Pty) Ltd 2006) 91
[745] M. Myers, Qualitative Research and the Generalizability Question: Standing Firm with Proteus, 4(3-4) The Qualitative Report 2000 <http://www.nova.edu/ssss/QR/QR4-3/myers.html> accessed 29th July 2015; V. Braun, V. Clarke, *Successful Qualitative Research: A Practical Guide for Beginners* (London, SAGE Publications Ltd 2013) 281

particular manner and clearly displaying the thought process.[746] Credibility was also aided through the use of well-established research methods; study of the culture of the organisation in which participants work before the interview; adoption of strategies to elicit honest responses; and numerous debriefing talks with supervisors.[747] Furthermore, the researcher asked the interview participants to review the transcripts.[748] Constant comparison were made, so that multiple perspectives were being communicated.[749] However, as observed by Yin trustworthiness is not achieved by following particular procedures[750] since "[a]ny prespecification of universal criteria is in danger of foisting on research artificial categories of judgment, and a framework of a prior conditions that may be impossible or inappropriate to meet..."[751]

Furthermore, reflexivity was employed and for this purpose knowledge was studied inwardly and outwardly i.e. the relationship between current knowledge and the knowledge gained from individual participants was studied.[752] Questions were asked as part of a critical appraisal, for instance, about the appropriateness of the sample in relation to the research objectives, the adequacy of the data collection and data analysis

[746] J. Morse, M. Barrett M, M. Mayan, K. Olson, J. Spiers, Verification strategies for establishing reliability validity in qualitative research, 1(2) *International Journal of Qualitative Methods* 2002, 1–19, 1-2; H. Noble, J. Smith, Issues of validity and reliability in qualitative research, 18(2) *Evidence-Based Nursing* 2015, 34-35

[747] A. K. Shenton, Strategies for ensuring trustworthiness in qualitative research projects, 22 *Education for Information* 2004, 63-75, 65-67

[748] T. Long, M. Johnson, Rigour, reliability and validity in qualitative research, 4 *Clinical Effectiveness in Nursing* 2000, 30-37; C. S. Ridenour, I. Newman, *Mixed Methods Research, Exploring the Interactive Continuum* (Southern Illinois University 2008) 40

[749] G. R. Gibbs, *Analysing Qualitative Data* (London, SAGE Publications Ltd 2007) 96

[750] R. K. Yin, *Qualitative Research from Start to Finish* (2nd ed, New York, The Guildford Press 2016) 86

[751] D. Garratt, P. Hodkinson, Can there be criteria for selecting research criteria? - A hermeneutical analysis of an inescapable dilemma, 4(3) *Qualitative Inquiry* 1998, 515-539, 533

[752] N. King, C. Horrocks, *Interviews in Qualitative Research* (London, SAGE Publications Ltd 2010) 125

process, the transferability of the research, and the adequacy of the ethical standards.[753] However, as the main approach is rooted in legal positivism, the qualitative data was unlikely to warrant an abrupt change, but rather provided insights which helped to fine-tune the findings.[754]

2.14 Data Analysis

The data was analysed and themes and patterns were identified, the data was grouped into categories.[755] The categories encapsulated the concepts and sub-concepts conveyed during the interviews.[756] This taxonomy started with bigger concepts which branched out into smaller sub-concepts, similar to a probability tree.[757] The researcher constantly compared the data, as advocated by proponents of grounded theory, such as Glasser and Strauss (1967).[758] For this purpose, the researcher read the transcripts, as well as the notes which were taken during the interviews.[759] Common characteristics which suggest that the data falls within a particular category or sub-category and particular concept were highlighted and a name was assigned, as well as distinct codes.[760] The data was thereby reduced and simplified.[761] The different codes were reviewed and scrutinised in

[753] A. Kuper, Critically appraising qualitative research, 33(7) *British Medical Journal* 2008 <http://www.bmj.com/content/337/bmj.a1035.full?ijkey=21e4db22678d417636de04f2b64921e4a58ffff0&keytype2=tf_ipsecsha> accessed 1st August 2015
[754] P. Leavy, *The Oxford Handbook of Qualitative Research* (Oxford, Oxford University Press 2014) 111
[755] L. Richard, *Handling Qualitative Data: A Practical Guide* (2nd ed, SAGE Publications Ltd 2009) 182
[756] P. Bazeley, *Qualitative Data Analysis: Practical Strategies* (London, SAGE 2013) 388
[757] Ibid
[758] B. Glaser, A. Strauss, *The discovery of grounded theory: Strategies for qualitative research* (London, Weidenfeld & Nicholson 1967) 1
[759] J. Y. Cho, E.-H. Lee, Reducing Confusion about Grounded Theory and Qualitative Content Analysis: Similarities and Differences, 19(16) *The Qualitative Report*, 1-20, 4
[760] S. M. Kolb, Grounded Theory and the Constant Comparative Method: Valid Research Strategies for Educators, 3(1) *Journal of Emerging Trends in Educational Research and Policy Studies* 2012, 83-86, 84
[761] Ibid

order to identify differences and similarities in a way which is integrated within the data set and clearly spelled out, so that it can be further tested.[762] When unique examples were provided, it was checked whether these fall into a particular category and if not a separate category was assigned. NVivo software was used and the search tools were employed to facilitate the data analysis process. Whenever a new node was created and the existing categories were changed, expanded or decreased, memos were made in order to stringently document the qualitative data analysis process. Whenever the researcher conducts a further interview, this process was repeated until no more categories could be identified and nodes could be assigned. The dominant topics thereby emerged. Statements were formulated and hypothesis were thereby generated i.e. an analytical induction process was employed.[763] The researcher assessed whether there were any negative cases or inconsistencies which contradicted particular hypothesis and constituted exceptions.[764] The NVivo program was used to graphically illustrate the main concepts and causal relationships.[765] Hence, a logical analysis was conducted.[766] Most fundamentally, the content was analysed, so that categories, concepts, themes and patters could be identified.[767] This necessitated ascertaining how often particular topics were being mentioned and analysing what matters were particular stressed or implicitly observed, reported and suggested.

---

[762] C. Conrad, A. Neumann, J. G. Haworth, P. Scott, *Qualitative research in higher education: Experiencing alternative perspective and approaches* (Needham Heights, Ginn Press 1993) 280
[763] S. J. Mangal, S. Mangal, *Research Methodology in Behavioural Sciences* (Delhi, PHI Learning Private Ltd 2013) 635
[764]S. M. Kolb, Grounded Theory and the Constant Comparative Method: Valid Research Strategies for Educators, 3(1) *Journal of Emerging Trends in Educational Research and Policy Studies* 2012, 83-86, 85
[765] G. Solinas, S. Vernizzi, Qualitative Tools of Strategic Analysis in (eds) A. B. Zanoni, *Strategic Analysis: Processes and Tools* (Abingdon, Routledge 2011) 34
[766] Also see R. G. A. Williams, Logical analysis as a qualitative method I: Themes in old age and chronic illness, 3(2) *Sociology of Health & Illness* 1981, 140-164, 140; M. Schreier, *Qualitative Content Analysis in Practice* (London, SAGE 2012) 241
[767] S. Elo, H. Kyngas, The qualitative content analysis process, 62(1*) Journal of Advanced Nursing* 2008, 107-115

Not only was a macro-analysis undertaken, but also a micro-analysis.[768] Once the content analysis was completed, the researcher looked at the frequencies by which particular topics and sub-topics were mentioned i.e. a small quantitative analysis approach was integrated within the qualitative data analysis process.[769] The researcher quoted what interview participants said, so that it was ensured that their point of view was portrayed in the manner in which they chose to communicate. These quotes were reported in such a way that the reader understands the context and cultural background in which they were made.[770] This is also known as a hermeneutical analysis, it ensured that the topic was much more elucidated and clarified and this resulted in a refined understanding of the core ideas conveyed by the text.[771] The information was narrated in a story-like manner, so that the language of the interviewee became understood.[772]

Emphasis was placed on how the interview participants experienced the topic of cybercrime and the researcher tried and viewed what was being reported through the lens of the interviewee.[773] Consequently, a phenomenological view point was adopted in order to ascertain the impact this has on the researcher, so that the data was interpreted

[768] E. Quimby, *Doing Qualitative Community Research, Lessons for Faculty, Students and Communities* (Brussels, Bentham Science Publishers 2012) 98
[769] M. B. Miles, A. M. Huberman, J. Saldana, *Qualitative Data Analysis: A Methods Sourcebook* (3rd ed, London SAGE 2014) 131
[770] U. Flick, *The SAGE Handbook of Qualitative Data Analysis* (London, SAGE Publications Ltd 2014) 235
[771] R. Tesch, *Qualitative Research: Analysis Types and Software: Analysis Types and Software Tools* (Abingdon, Routledge 1990) 94
[772] C. Grbich, *Qualitative Data Analysis: An Introduction* (2nd ed, London, SAGE Publications Ltd 2013) 227
[773] D. E. Polkinghorne, Narrative configuration in qualitative analysis
Narrative configuration in qualitative analysis, 8(1) *International Journal of Qualitative Studies in Education* 1995, 5-23, 5

heuristically.[774] The triangulation of the legal methods data formed part of the discussion of the interview results.

2.15 Publishing Qualitative Research

The research was privately funded, though due to the researcher's position as a judge, it was easy to gain access and also because of the interest in the research phenomenon. It is therefore hoped that the research is of use to the judiciary and legislators. Whilst the research benefits the judiciary and the legislator in the UAE, the research also benefits other countries which are developing their legal framework to combat cybercrime. The researcher therefore intends to attend conferences in order to exchange views with peers and hopes to also publish articles about his findings. When articles will be published and/or findings will be presented at conferences, great care will be taken to keep the names of interview participants anonymous, including by removing other identifiers, as discussed above. As the research deals with cybercrime which is critical to the security of the nation, it will be ensured that no harm emanates as a result of the research findings, for instance, by revealing insider information.

2.16 Summary

The research is situated within paradigms: Firstly and predominantly the research is rooted in legal positivism and is therefore rooted in realism, functionalism and

[774] G. Kleining, H. Witt, The Qualitative Heuristic Approach: A Methodology for Discovery in Psychology and the Social Sciences. Rediscovering the Method of Introspection as an Example, 1(13) *Qualitative Social Research* 2000 <http://www.qualitative-research.net/index.php/fqs/article/view/1123/2495> accessed 15th July 2015

empiricism making use of a nomothetic methodology. Secondly, the research is interpretivist and therefore perceives existence from the viewpoint of epistemic relativism and through an ideographic lens which is inherently nominalistic and phenomenological, and meanings are therefore understood through hermeneutics. In line with the ontological orientation, the researcher counted as knowledge not only objective facts, for instance, valid laws, but also subjective experiences of individuals and therefore recognised that knowledge can be acquired through the study of individual opinions and expressions. By looking at the issue from the paradigm of positivism and the opposing paradigm of interpretivism, questions which could not be answered by one empirical strategy could be successfully addressed by the other empirical tactic.[775] Furthermore, it made it possible to shift from theory to observation and back, and thereby avoided that the legal positivist findings became overtly rigid since the perceptions of individuals were taken into account, resulting in more integrated, holistic and diverse findings.[776] This is because different paradigms capture a different perspective of reality and therefore of the research phenomenon.[777] A pragmatic approach was thus adopted in order to creatively combine the positivist with the interpretivist approach, thereby minimising the weaknesses of both paradigms and maximising their benefits.[778] By combining both approaches, theory, practice and reflection were brought together, which assisted with questioning existing laws and assumptions.

---

[775] W. J. González, *New Methodological Perspectives on Observation and Experimentation in Science* (La Coruna, Netbiblo 2010) 180
[776] Ibid
[777] J. E. M. Sale, L. H. Lohfeld, K. Brazil, Revisiting the Quantitative-Qualitative Debate: Implications for Mixed-Methods Research, 36 *Quality & Quantity* 2002, 43-53
[778] D. Ary, L. Cheser Jacobs, C. Sorensen, A. Razvieh, *Introduction to Research in Education* (8th edn, Belmont, Wadsworth Cengage Learning) 559

Inductive reasoning was particularly employed, and hypotheses were developed based on the literature, though also deductive logic was employed in respect of the data generated from the interviews. Whilst the quantitative parts dealt with the particular laws, the qualitative parts focused more broadly on understanding the research phenomenon outside the narrow prescriptions of the law and looked at the practical effects.

Furthermore, it has been discussed that three methods were used, namely: the black letter law approach; the comparative method; and a qualitative study employing the interview guide approach. For the doctrinal legal analysis all relevant primary and secondary sources were studied. The comparative method compared the laws in the UAE, the UK and the European Union, particularly with a view of highlighting differences and similarities. Hence, the research explored how e-crime legislation in these different jurisdictions addressed the issue of cybercrime. Additionally, the empirical method was used to assess the impact of the law. It was assumed that the research problem is better understood by adopting a mixed method research strategy, as opposed to adopting a purist stance solely rooted in black letter law.

As the researcher therefore employed the qualitative social science research method, it was pertinent that he safeguarded research participants from any harm which may arise due to the sensitivity of the research topic. The highest ethical standards were therefore displayed. The anonymity of the interviewees was preserved. The semi-structured interview method was employed in order to elicit maximum understanding about the research topic. Non-probability purposive sampling was employed to ensure that rich

and thick data was generated. The face-to-face interviews were held in a private setting. The interviews were immediately translated and transcribed. A thorough research process was followed in order to achieve data quality. The same interview questions were asked, clear research procedures were followed, opinions were not generalised, but differences were pointed out. An accurate account was provided of what was being reported. In-depth descriptions were provided, and it was explained which themes emerged from the findings and these were broadly captured. Various steps were taken to enhance trustworthiness, for instance, accurate records were kept. Credibility was also established through the use of recognised research methods. Furthermore, the researcher adopted a reflexive process i.e. examined his own beliefs and assumptions and how these impacted the findings. The qualitative data was coded with the help of NVivo software in order to identify categories, concepts, themes and patterns and a small quantitative analysis was also conducted i.e. it was analysed how often certain categories, concepts, themes and patterns were mentioned. The researcher intends to publish articles about his findings and will take great care to ensure the anonymity of all research participants.

The next chapter critically discusses the theoretical context by examining the UK's main computer misuse offences, RIPA policing powers, data retention and public interest immunity.

Chapter Three: The UK's Main Computer Misuse Offences, RIPA Policing Powers, Data Retention and Public Interest Immunity

3. Introduction

For cybercrime to be combated, the first step is to enact a law which criminalises deviant behaviour. In light of innovation, it has to be also ensured that the law is kept up to date. This Chapter will therefore start with an analysis of the promulgation and enactment of the Computer Misuse Act 1990 and its legislative history in terms of subsequent amendments. The passing of cybercrime laws is one step, but for enforcement agencies to be able to prevent, detect and prosecute cyber-criminals, it is essential that they are equipped with the necessary powers. In the UK, enforcement agencies have been permitted to intercept communications data, engage in surveillance and to acquire communications data and to decrypt communications data when it has been encrypted. Yet it is vital that a due process is followed, so that these powers are not abused,the rule of law is upheld and fundamental rights and freedoms are not unduly curtailed. The Chapter will therefore scrutinise the powers which RIPA confers in terms of interception, surveillance, communications data acquisition and decryption and its governing framework. A related issue is the topic of data retention, so that enforcement agents can look at historic data when they are investigating a crime. The EU approach towards data retention will therefore be analysed, including the now defunct Data Retention Directive, the Grand Chamber decision of the Court of Justice of the

European Union in which this Directive was declared invalid, as well as the UK's emergency legislation which was passed in response to this, as well as the Investigatory Powers Act 2016 which replaced the emergency legislation. Finally, the chapter discusses the UK prohibition which renders intercepted communication inadmissible in court proceedings.

3.1 The Computer Misuse Act 1990

Prior to the enactment of the Computer Misuse Act 1990, computer crime was purely governed by criminal law, and more specifically the Criminal Damage Act of 1971[779], this has now hanged as the government has enhanced the legal principles governing and regulating computer crime through the enactment of the Computer Misuse Act 1990, which now governs computer crime in conjunction with the Criminal Damage Act 1971. The two acts were considered in conjunction in the 1991 case of *R v Whiteley*[780], clarifying in this way that the Criminal Damage Act 1971 will still be applicable despite the enactment of the Computer Misuse Act 1990. For example, s.1(1) of the Criminal Damage Act 1971 covers situations when computer data, which was stored on a magnetic disk, was erased.[781] S.1(1) of the Criminal Damage Act 1971 provides:

> *"A person who without lawful excuse destroys or damages any physical property belonging to another, intending to destroy or damage such property or being reckless as to whether any such property would be destroyed or damaged shall be guilty of an offence."*

[779] C. Tapper, 'Computer crime: Scotch mist?' (1987) *Criminal Law Review* 4
[780] *R v Whiteley (1991) 93 Cr. App. R. 25*

[781] S. Fafinski, *Computer Misuse: Response, Regulation and the Law* (Abingdon, Routledge 2014) 22

However, the issue was that it required a creative interpretation in order to demonstrate that tangible property had been physically damaged.[782] In *R v Talboys*[783], a person escaped a charge for a programming prank. In *Cox v Riley*[784], a person was charged with erasing computer programs from a plastic circuit card. The saw was thereby rendered inoperable. The defendant appealed on the basis that the programs, which he erased, did not constitute tangible property. The Divisional Court found that this constituted damage. In 1988, the Law Commission published a Working Paper on Computer Misuse, which observed:

> *"[i]n essence, any interference with the operation of a computer or its software which causes loss or inconvenience to its legitimate users can probably now be charged as criminal damage...The law of criminal damage now seems to extend to persons who damage a computer system, without the need for any further reform of the law."*[785]

In 1989, the Law Commission then published a Final Report on Computer Misuse, which highlighted the issues and stated:

> *"the police and prosecuting authorities who have informed us that, although convictions have been obtained in serious cases of unauthorised access to*

[782] Ibid
[783] The Times 29 May 1986
[784] (1986) 83 Cr App R 54
[785] Law Commission, Computer Misuse (Working Paper No.110, 1988) paras3.35&3.68; S. Fafinski, *Computer Misuse: Response, Regulation and the Law* (Abingdon, Routledge 2014) 22

data or programs, there is recurrent (and understandable) difficulty in explaining to judges, magistrates and juries how the facts fit in with the present law of criminal damage."[786]

The following year, the Computer Misuse Act 1990 was enacted expressly for the purpose of combating computer hacking.[787] Various anti-hacking offences were enacted, namely to gain unauthorised access to computer material (ss1 and 2); to modify computer material without authorisation and to access with an intention to facilitate or perpetrate offences without authorisation (s.3).[788] S.1 of the Computer Misuse Act 1990 is a key element as it links to other provisions, including s.2, as discussed below. For this reason, Lloyds describes it as *"the most critical element of the legislation."*[789] S.1 of the Computer Misuse Act 1990 states:

"1. A person is guilty of an offence if –

(a) he causes a computer to perform any function with intent to secure access to any program or data held in any computer;

(b) the access he intends to secure is unauthorized; and

(c) he knows at the time when he causes the computer to perform the function that that is the case."

[786] Law Commission, Computer Misuse, 1989, para.2.31; I. J. Lloyd, *Information Technology Law* (6th ed, Oxford, Oxford University Press 2011) 233
[787] M. Chesher, R. Kaura, P. Linton, *Electronic Business & Commerce* (London, Springer 2003) 326
[788] A. Jain, *Cybercrime: Cybercrime: Issues and Threats and Management* (Delhi, Isha Books 2005) 105
[789] I. J. Lloyd, *Cyber Law in the United Kingdom* (AH Alphne aan den Rijn, Kluwer Law International 2010) 199

Although, the technical terms are not defined, it is clear that three aspects require close consideration:[790] Firstly, what can constitute access is very broad. Secondly, it has to be determined whether access was unauthorised. Thirdly, the level of intent which has to be shown to exist is relevant for being prosecuted under s.1. The *actus reus* requirement to establish the offence is satisfied when a computer is used i.e. a person *"causes a computer to perform any function."*[791] The definition to *"perform any function with intent to secure access"* covers any act where a computer is used.[792]

The statute omits to define what a computer is, which is good, as technology is constantly evolving and as a result, any device, which can store data electronically, including mobile phones or smart watches, can be a computer.[793] Lord Hoffman adopted a flexible interpretation when he stated that a computer is *"a device for storing, processing and retrieving information."*[794] Any other interpretation would result in many cybercrime offences escaping punishment.[795] The *mens rea* for the offences is to have an intention to gain access to some data regardless of whether or not it can be identified which item the defendant sought to gain access to.[796] Hence, those who engaged in searching for a program or file can possess the requisite *mens rea*.[797]

---

[790] I. J. Lloyd, *Cyber Law in the United Kingdom* (AH Alphne aan den Rijn, Kluwer Law International 2010) 199
[791] S. Hedley, *The Law of Electronic Commerce and the Internet in the UK and Ireland* (London, Cavendish Publishing Ltd 2006) 18
[792] I. J. Lloyd, *Cyber Law in the United Kingdom* (AH Alphne aan den Rijn, Kluwer Law International 2010) 199-200
[793] S. Hedley, *The Law of Electronic Commerce and the Internet in the UK and Ireland* (London, Cavendish Publishing Ltd 2006) 18
[794] *DPP v McKeown; DPP v Jones* (1997) 1 WLR 295, per Lord Hoffman at 302; S. Fafinski, *Computer Misuse: Response, Regulation and the Law* (Abingdon, Routledge 2014) 36
[795] S. Hedley, *The Law of Electronic Commerce and the Internet in the UK and Ireland* (London, Cavendish Publishing Ltd 2006) 18
[796] S.1(2) of the Computer Misuse Act 1990; ibid (Hedley) 18
[797] ibid (Hedley) 18

A problem arose in *R v Cropp*[798], as Aglionby J considered that *"[i]t seems to me, doing the best that I can in elucidating the meaning of section 1(1)(a) [of the Computer Misuse Act 1990], that a second computer must be involved. It seems to me to be straining language to say that only one computer is necessary..."*[799] Equally, in *A-G's Reference (No.1 of 1991)*[800], it was suggested that two computers are required i.e. one to perform the function and another one to access any data or program. However, the court found that one machine is sufficient to establish both aspects.[801] Lord Taylor of Gosforth CJ explained that otherwise the Act would have left a gap, *"as going straight to the in-house computer and extracting confidential information from it could be committed with impunity so far as the three offences in this Act are concerned."*[802]

In *DPP v Bignell,* [803] a married couple, who were both police officers, obtained information about the ex-wife of the husband. They were charged under s.1, but appealed on the basis that they accessed the data lawfully, as they had authority to access the police national computer. Yet they acknowledged that this was for a purpose which was unauthorised. Astill J held that the Computer Misuse Act 1990 was adopted to combat hacking and breaking into computer systems.[804] He therefore concluded that as they were police officers, they had authority to access the police national computer and therefore did not act in a manner which was unlawful. Lloyd observes that the

[798] (unreported) 4 July 1990
[799] Cited from S. Fafinski, *Computer Misuse: Response, Regulation and the Law* (Abingdon, Routledge 2014) 52
[800] (1993) QB 94
[801] S. Hedley, *The Law of Electronic Commerce and the Internet in the UK and Ireland* (London, Cavendish Publishing Ltd 2006) 18
[802] *A-G's Reference (No.1 of 1991)* (1993) QB 94, per Lord Taylor of Gosforth CJ at 100
[803] (1998) 1 Cr App R 1
[804] *DPP v Bignell* (1998) 1 Cr App R 1, at 12

adoption of Astill J's approach would have had serious repercussions for the Computer Misuse Act 1990.[805] This is because a lot of cybercrime is perpetrated by insiders or employees.[806] Similarly, Wasik criticises the decision, as authorisation for a lawful purpose should not be equated with having lawful authority for a non-legitimate purpose.[807]

The House of Lords subsequently rejected this approach in *R v Bow Street Magistrates' Court, ex parte Allison*[808], where it was made clear that misutilising access rights could result in criminal sanctions. The House of Lords pointed out that in *DPP v Bignell,*[809] the court had mistaken the concept of being allowed to access a network or computer with being allowed to access data and programs.[810] Lord Hobhouse explained that s.17 of the Computer Misuse Act 1990 sets out what the concepts of access and authorisation denote. S.17(2)(a)-(s) makes clear that access to data or a program is shown to have gained when a user causes the computer to erase or alter, move or copy to a different location, use or output it by displaying it or in any other form.[811] S.17(3)(a)(b) provides that access is gained to a program if the person *"causes the program to be executed"*; or *"is itself a function of the program."* Hence, when a program is run, then access is gained.[812] With this definition, most actions which result in a user using a computer

[805] I. J. Lloyd, *Cyber Law in the United Kingdom* (AH Alphen aan den Rijn, Kluwer Law International 2010) 200
[806] Ibid
[807] M. Wasik, 'Computer misuse and misconduct in public office' (2008) 22 *International Review of Law, Computers and Technology*, 135, 137
[808] (1999) 4 All ER 1
[809] (1998) 1 Cr App R 1
[810] S. Fafinski, *Computer Misuse: Response, Regulation and the Law* (Abingdon, Routledge 2014) 56
[811] S.17(2)(a)-(d) of the Computer Misuse Act 1990
[812] S. Hedley, *The Law of Electronic Commerce and the Internet in the UK and Ireland* (London, Cavendish Publishing Ltd 2006) 18

system and the system showing or transmitting information will be covered by the Computer Misuse Act 1990.[813]

Moreover, s.17(5)(a)-(b) explains that any kind of access which a person gains to data or a program is unauthorised if the person is not allowed to control access to the data or program; and the person who is entitled to control access has not consented that s/he can access the data or program. In *R v Bow Street Magistrates' Court, ex parte Allison,*[814] it was also made clear that when an employee's authorisation to access data is limited, but he nonetheless exceeds this, then this may fall within the scope of the Computer Misuse Act 1990. Stein states that this was seen as the Act coming of age, thereby enabling authorities to fully utilise the Act.[815]

For a s.2 charge to be made out, the requisite elements, which have to be satisfied, are to commit a s.1 offence and to show that there is an intention to facilitate or commit a *"further"* offence, which is of a more serious kind. Further offences are those where *"the sentence is fixed by law"* or where a person is over eighteen and has not been previously convicted for a charge for five years.[816] However, it does not have to be shown that this further offence has been carried out.[817] Examples where s.2 offences may be committed are intending to commit theft, for instance, by channelling funds during an online transfer to a different account or accessing sensitive information in

[813] I. J. Lloyd, *Cyber Law in the United Kingdom* (AH Alphne aan den Rijn, Kluwer Law International 2010) 199-200
[814] (1999) 4 All ER 1
[815] K. Stein, 'Unauthorised access' and the UK Computer Misuse Act 1990: House of Lords 'leaves no room' for ambiguity' (2006) 6 *Computer and Telecommunications Law Review* 63, 63; S. Fafinski, *Computer Misuse: Response, Regulation and the Law* (Abingdon, Routledge 2014) 57
[816] S.2(2) of the Computer Misuse Act 1990
[817] D. Omerod, *Blackstone's Criminal Practice 2012* (Oxford, Oxford University Press 2011) 908

order to blackmail a person with the information.[818] Moreover, a person can intend to perpetrate this further offence at the same time the s.1 offence is being committed.[819] A person can be charged even if it was not possible to commit the further offence.[820] Omerod explains that this corresponds with the rule in s.1(2) of the Criminal Attempts Act 1981.[821]

In 2004, the All Party Parliamentary Internet Group suggested that the Computer Misuse Act 1990 should be revised.[822] The Police and Justice Act 2006, Part 5 then made various amendments, which were designed to address issues with the Computer Misuse Act 1990, especially in respect of DoS attacks and to ensure compliance with the Cybercrime Convention.[823] S.3 of the Computer Misuse Act 1990, which deals with causing unauthorised modifications to data or programs stored on a computer, was amended by virtue of the Police and Justice Act 2006. S.3 is entitled *"Unauthorised acts with intent to impair, or with recklessness as to impairing, operation of computer, etc."* and s3(1) states that:

> *"[a] person is guilty of an offence if –*
>
> *(a) he does any unauthorised act in relation to a computer;*
>
> *(b) at the time when he does the act he knows that it is unauthorised; and*

[818] Ibid
[819] S.2(3) of the Computer Misuse Act 1990
[820] S.2(4) of the Computer Misuse Act 1990
[821] Also see *R v Shivpuri* (1987) AC 1; D. Omerod, *Blackstone's Criminal Practice 2012* (Oxford, Oxford University Press 2011) 908
[822] All Party Parliamentary Internet Group, Revision of the Computer Act, 2004
[823] J. Clough, *Principles of Cybercrime* (2nd ed, Cambridge, Cambridge University Press 2015) 53-54

a person convicted of the offence may be sentenced to a maximum of 12 months' imprisonment on summary conviction (6 months in Scotland) or ten years on indictment."

Erasing, altering or adding data all constitute an unauthorised act.[824] When a person modifies data, then this is considered unauthorised if the person who was entitled to consent has not permitted this or the person who did the act had no such authority.[825] S.3(2) makes clear that an unauthorised act has:

"(a) to impair the operation of any computer;

(b) to prevent or hinder access to any program or data held in any computer; [or]

(c) to impair the operation of any such program or the reliability of any such data; [or

(d) to enable any of the things mentioned in paragraphs (a) to (c) above to be done."

Moreover, s.3(5)(c) further provides that *"impairing, preventing or hindering"* can include temporary acts. S.3(4) also states that the intention does not have to relate to:

"(a) any particular computer;

(b) any particular program or data; or

[824] S.17 of the Computer Misuse Act 1990
[825] S.17 of the Computer Misuse Act 1990

(c) a program or data of any particular kind."

Consequently, a person, who creates a virus, which causes that a computer is modified, can be held responsible, despite the person not being responsible for a particular device, as this may even be caused by an authorised user, who is unaware of the virus.[826] Accordingly, *"causing"* means acts which have a particular effect and acts where there is proximity with the effect.[827]

The amendment of s.3 ensures compliance with Article 3 of the Cybercrime Convention, which states that:

> *"1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right.*
>
> *2. A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm."*

Furthermore, Article 5 of the Cybercrime Convention was taken into account,[828] it states that:

> *"Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when*

[826] I. J. Lloyd, *Information Technology Law* (7th ed, Oxford, Oxford University Press 2014) 214
[827] Ibid
[828] Ibid, 212

committed intentionally, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data."

Prior to the amendment, it had to be shown that the person had the intention, but the Police and Justice Act 2006 has lowered the threshold in respect of s.3, so that the *mens rea* is acting intentional or being reckless in respect of causing the impairment.[829] For instance, s.3 renders it illegal to intentionally delete data or programs or to input additional data into the computer system or to infect a computer with a virus or to install a program which causes a disturbance.[830] S.3 also renders it illegal to access a cable television channel without a subscription[831] or to interfere with a website.[832]

An example of a case under s.3 is that of *R v Whitaker,*[833] where the person was charged with installing a program which prevented the use of a computer, except when a password was used.[834] However, the password was not provided and the computer could not be used for a period of time, which resulted in losses.[835] In *DPP v Lennon,*[836] a former employee was charged under s.3, who was disgruntled and had impaired the employer's computer and thereby ensured that the company received 5 million emails. The Court did not accept that the defence in s.17(8)(b) of the Computer Misuse Act

[829] Ibid, 213
[830] Ibid
[831] *R v Parr-Moore* (2003) 1 Cr App R (S) 425 (CA)
[832] *R v Lindesay* (2002) 1 Cr App R (S) 270 (CA); S. Fafinski, *Computer Misuse: Response, Regulation and the Law* (Abingdon, Routledge 2014) 41
[833] (1993) unreported (Scunthorpe Magistrates' Court)
[834] R. Battcock, 'Prosecutions under the Computer Misuse Act' (1996) *Computers and Law* 6, 22
[835] Ibid
[836] (2006) 170 JP 532

1990 could be evoked, as consenting to receive emails was not unlimited. Following the introduction of the Computer Misuse Act 1990 it was becoming apparent, over time, that the act was insufficient in dealing with new manifestations of computer misuse that were unknown and unforeseen at the time of its enactment, therefore a change was vital, hence for the amendments introduced by the Police and Justice Act 2006.[837]

Apart from the amendment of s.3, the other main changes which were introduced by virtue of sections 35-38 of the Police and Justice Act 2006 were as follows:[838] The maximum sentence was increased to two years for the s.1 of the Computer Misuse Act 1990 offence (i.e. to gain unauthorised access to computer material).[839] In respect of s.3 offences (i.e. to try and impair the way a computer operates without authority) the maximum sentence was increased to ten years.[840] Additionally, a new offence was created which was added as s.3A to the Computer Misuse Act 1990, which outlaws that articles are made, supplied or obtained which are used for the purpose of computer misuse crimes.[841] In 2007/2008, the House of Lords Science & Technology Committee dealt with the issue whether the s.3A offence would result in those, which develop tools to perpetrate offences, e.g. security testers, committing an offence. The Crown Prosecution Service (CPS) guidance clarified that such tools could be used for

[837] Stefan Fafinski, (2006) 'Access Denied: Computer Misuse in an Era of Technological Change' 70 JCL 424.
[838] Secretary of State for the Home Department, Memorandum to the Home Affairs Committee, Post-legislative assessment of the Police and Justice Act 2006, Cm 8195, October 2011, 1-32, 21, para.108 <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/229021/8195.pdf> accessed 14th November 2015
[839] Ibid
[840] Ibid
[841] Ibid

authorised purposes.[842] The amendments and more specifically s.3 have opened up a 'range of potential interpretative challenges that may trouble both security professionals and the courts'[843]

In 2015, further changes were made to the Computer Misuse Act 1990 by virtue of s.41(2) of the Serious Crime Act 2015 which *"updates the existing offences to cover importing tools for cybercrime (such as data programmes designed for unlawfully accessing a computer system."*[844] This also achieves compliance with Article 7 of the Directive 2013/40/EU on attacks against information systems. This Article requires that Member States render it illegal to interfere with systems; to illegally intercept; or to gain illegal access. Equally, the tools, which are used to commit offences, are rendered illegal when there is an intention to produce, sell, procure for import, use, distribute or otherwise make available these tools without being entitled to commit any of the offences set out in Article 3 to 6 of the Directive.[845] The criminal offence is not minor where there is a computer programme which is designed to commit the offences or the tool is designed to obtain access codes, computer passwords or comparable data, so that an information system can be accessed.[846] The Explanatory Notes state that s.3A of the Computer Misuse Act 1990 complies with Article 7 of the Directive, together with

[842] Ibid, 21-22, para.109
[843] Stefan Fafinski, (2008) 'Computer misuse: the implications of the Police and Justice Act 2006' Journal of Criminal Law 72(1), 53-66.

[844] Serious Crime Act 2015, Explanatory Notes <http://www.legislation.gov.uk/ukpga/2015/9/notes> accessed 1st December 2015
[845] Article 7 of the Directive 2013/40/EU on attacks against information systems
[846] Serious Crime Act 2015, Explanatory Notes, para.134
<http://www.legislation.gov.uk/ukpga/2015/9/notes> accessed 1st December 2015

sections 1 to 3, except in relation to procuring use of tools. S.3A of the Computer Misuse Act 1990 is therefore amended to:

> *"a person is guilty of an offence if he obtains any article with a view to article –*
>
> *(a) intending to use it to commit, or assist in the commission of, an offence under section 1, 3 or 3ZA, or*
>
> *(b) with a view to its being supplied for use to commit, or assist in the commission of, an offence under section 1 or 3."*[847]

The Serious Crime Act 2015 also introduces a new s.3ZA entitled *"unauthorised acts causing, or creating risk of, serious damage"*, which can result in a fine and imprisonment of up to 14 years or life imprisonment.[848] S.3ZA ensures that computer hacking which causes serious damage to the national security of any country, the UK economy, the environment or human welfare is rendered illegal.[849] This ensures that the UK complies with Directive 2013/40/EU on attacks against information systems.[850] The government also considered that there was a gap within the criminal law, as the most serious hacking offence of impairing the way in which a computer operates without authorisation under s.3 only carries a maximum sentence of up to ten years in prison, but

---

[847] Serious Crime Act 2015, Explanatory Notes, para.135 <http://www.legislation.gov.uk/ukpga/2015/9/notes> accessed 1st December 2015

[848] House of Lords, *House of Commons, Joint Committee on Human Rights, Legislative Scrutiny: (1) Serious Crime Bill, (2) Criminal Justice and Courts Bill (second Report) and (3) Armed Forces (service Complaints and Financial Assistance) Bill, Second Report of Session 2014-15. HL Paper 49, HC 746* (London, the Stationery Office Ltd 2014) 8

[849] S.3ZA of the Computer Misuse Act 1990

[850] S. Summers, C. Schwarzenegger, G. Ege, F. Young, *The Emergence of EU Criminal Law: Cybercrime and the Regulation of the Information Society* (Oxford, Hart Publishing 2014) 69

this was deemed insufficient.[851] The adoption of the new section is crucial in order to protect critical infrastructures from cyber attacks, but the Joint Committee on Human Rights observes that it is not certain what *"damage to the economy", "damage to the environment"* or *"damage to national security"* or *"damage to human welfare"* mean in order to justify a sentence of up to 14 years or life imprisonment.[852] They state that the Act *"therefore appears to cross a significant line by using these unsatisfactory concepts in the definition of a serious criminal offence carrying a lengthy sentence."*[853] It is therefore important that these terms are defined.

Moreover, as the digital space has no national borders, it is important that this issue is addressed.[854] The Computer Misuse Act 1990 therefore allows for extra-territorial jurisdiction to a limited extent in respect of the offences detailed in sections 1 and 3.[855] Orakhelashvili observes that the UK is one of the few countries, which have adopted *"technology-specific jurisdiction"* in ss4-5 i.e. requires that there is a significant link with the domestic jurisdiction.[856] Additionally, s.6 details the jurisdiction for inchoate offences, such as conspiracy and attempt, when there is computer misuse.[857]

Article 12 of Directive 2013/40/EU on attacks against information systems makes provisions in respect of jurisdiction.[858] Article 12(1) requires that jurisdiction should be

---

[851] House of Lords, *House of Commons, Joint Committee on Human Rights, Legislative Scrutiny: (1) Serious Crime Bill, (2) Criminal Justice and Courts Bill (second Report) and (3) Armed Forces (service Complaints and Financial Assistance) Bill, Second Report of Session 2014-15. HL Paper 49, HC 746* (London, the Stationery Office Ltd 2014) 8-9
[852] Ibid, 11
[853] Ibid
[854] Alisdair A. Gillespie, *Cybercrime: Key Issues and Debates* (Abingdon, Routledge 2016) 25
[855] Sections 4-5 of the Computer Misuse Act 1990; United Nations Conference on Trade and Development, *Information Economy Report 2005* (New York, United Nations 2005) 12
[856] A. Orakhelashvili, *Research Handbook on Jurisdiction and Immunities in International Law* (Cheltenham, Edward Elgar Publishing Ltd 2015) 53
[857] D. Omerod, *Blackstone's Criminal Practice 2012* (Oxford, Oxford University Press 2011) 911
[858] Serious Crime Act 2015, Explanatory Notes, para.136 <http://www.legislation.gov.uk/ukpga/2015/9/notes> accessed 1st December 2015

established when Articles 3 to 8 offences are committed *"(a) in whole or in part within their territory; or (b) by one of their nationals, at least in cases where the act is an offence where it was committed."* Article 12(2)(a)(b) requires that in respect of Article 12(1)(1)(a) jurisdiction has to be established when the offender is present in the territory of the Member State, though the offence is committed against an information system or the offence takes place in the territory of the Member States, even though the offender is not present in the territory of the Member State. Sections 4 and 5 of the Computer Misuse Act 1990 already grant jurisdiction when there is a *"significant link"* to the relevant jurisdiction. Nonetheless, s.4(2) is amended, so that extra-territorial jurisdiction can be established in respect of the new s.3ZA.[859] Equally, s.5 is revised, so that it is defined what a *"significant link"* is.[860] As a result, it is, for example, possible to convict an Italian national, who resides in England and hacks computer systems in Italy or a UK national, who hacks computer systems in the UK, whilst he resides in Italy and then returns to the UK.[861] Furthermore, a new s.5(1a) and (1B) make it possible to prosecute UK nationals, even though the offence has no significant link to the UK, so long as the offence is one in the country where the person resides.[862]

The Computer Misuse Act 1990 remains the main statute for pursuing cybercrime and the improved Act ensures that also those, who make, supply and use tools to perpetrate offences set out in the Computer Misuse Act can be prosecuted.[863] As mentioned in

---

[859] Serious Crime Act 2015, Explanatory Notes, para.137 <http://www.legislation.gov.uk/ukpga/2015/9/notes> accessed 1st December 2015
[860] Ibid
[861] Ibid
[862] Ibid, para.138
[863] Secretary of State for the Home Department, Memorandum to the Home Affairs Committee, Post-legislative assessment of the Police and Justice Act 2006, Cm 8195, October 2011, 1-32, 22, para.110 <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/229021/8195.pdf> accessed 14th November 2015

Chapter One, reliance can additionally be placed on other legislation, such as the Protection of Children Act 1978, the Protection from Harassment Act 1997, the Sexual Offences Act 2003. Despite the Computer Misuse Act 1990 having been adopted, the prevention, detection and prosecution of cyber criminals for these offences is difficult and it is important that enforcement agencies are equipped with powers to conduct surveillance of the online space, so that business and individuals can use it safely, which is discussed next.[864]Neil Mac Ewan contends that the even though the changes should be welcomed as they do cause some improvement *'the new provisions will also bring some problems of their own. A combination of some short-sighted, or simply stubborn, policy-making and some forceful government amendment during the Bill's passage through Parliament has produced certain provisions which invite controversy, could sometimes prove difficult to interpret or enforce, and may lead to claims of legislative overkill.'*[865]

3.2 Interception, Surveillance, Communications Data Acquisition and Decryption and the UK Regulation of Investigatory Powers Act 2000 (RIPA)

In the 1960s, British police undertook the first experiments with CCTV in Liverpool and London.[866] Since then new technological innovations have transformed the *"crime control field"* in line with broader global trends in response to terrorism.[867] Furthermore,

[864] D. Thomas, B. D. Loader, 'Cybercrime: law enforcement, security and surveillance in the information age' in (eds) B. D. Loader, D. Thomas, *Cybercrime: Security and Surveillance in the Information Age* (Abingdon, Routledge 2005) 1
[865] Neil MacEwan, (2008) The Computer Misuse Act 1990: lessons from its past and predictions for its future Criminal Law Review 12, 955-967.

[866] C. A. Williams, 'Police Surveillance and the Emergence of CCTV in the 1960s' (2003) 5 *Crime Prevention and Community Safety: An International Journal*, 27-37, 27
[867] M. McCahill, 'Theorizing Surveillance in the UK Crime Control Field' (2015) 3(2) *Open Access Journal*, 10-20, 10

in an information society, intelligence-led policing has increasingly been adopted as a management model for enforcement agencies.[868] Intelligence and its analysis are therefore considered essential to prevent, detect and investigate cybercrime.[869] This necessitates that surveillance takes place and communications are intercepted and data is acquired and encrypted data can be decrypted.[870]

In the past, interception meant opening letters or reading private telegrams, but in a digital world new techniques have been adopted, including in respect of communications data.[871] Haggerty and Ericson define surveillance as the *"collection and analysis of information about populations in order to govern their activities."*[872] Communications data can be divided into three types: traffic data; use data; and subscriber data.[873] Subscriber data is information which the service provider holds i.e. the person's name and contact details; use data consist of itemised records, e.g. of online calls; and traffic data is information which is attached to the communication and informs e.g. about the location.[874]

A multitude of new procedures have been adopted by the state to gather, control and manage information. State agencies have been equipped with comprehensive and invasive power to collect information about its citizens.[875] As a result, the population is

---

[868] Ibid
[869] P. Gottshalk, *Policing Cybercrime* (Ventus Publishing ApS 2010) 98
[870] Ibid, 101
[871] S. Foster, *The Judiciary, Civil Liberties and Human Rights* (Edinburgh, Edinburgh University Press 2006) 141
[872] K. D. Haggerty, R. V. Ericson, 'The new politics of surveillance and visibility' in (eds) K. D. Haggerty and R. V. Ericson, *The new politics of surveillance and visibility* (Toronto, University of Toronto Press 2006) 3
[873] Secretary of State for the Home Department, *Draft Communications Data Bill, Cm 8359* (London, TSO Shop Ltd 2012) 14
[874] Ibid
[875] M. O'Neil, B. Loftus, 'Policing and the surveillance of the marginal: Everyday contexts of social control' (2013) 17(4) *Theoretical Criminology*, 437-454, 437

directly supervised.[876] What began with photographs and fingerprints has transformed into surveillance cameras, computer databases and other new sophisticated surveillance technology.[877] In the UK, the *"processes of normalisation of surveillance have gone much further than elsewhere."*[878] Tempora[879] was used by GHCQ to tap fibre-optic cables in order to conduct internet surveillance.[880] Additionally, the clandestine US's PRISM programme operated by the US National Security Agency (NSA) has been accessed by the UK intelligence service in order to monitor British people in addition to the operation of the domestic surveillance regime, for instance, as spelled out in RIPA. [881] The abovementioned mass-surveillance systems came to light after the revelations by Edward Snowden, and it has been argued that the cabinet was not aware of these systems[882], having in mind the secret nature of these systems, as well as the major interference they allegedly have in the lives of civilians, it is not surprising UK

[876] M. McCahill, 'Theorizing Surveillance in the UK Crime Control Field' (2015) 3(2) *Open Access Journal*, 10-20, 10

[877] G. T. Marx, 'What's new about the new surveillance? Classifying for change and continuity' (2002) 1(1) *Surveillance and Society*, 9-29, 11

[878] D. Murakami Wood, W. Webster, 'Living in surveillance societies: The normalisation of surveillance in Europe' (2009) 5(2) *Journal of Contemporary European Research*, 259-273, 260

[879] Tempora is the name of a programme under which data inceptors were placed on fibre-optic transatlantic cables which carry internet traffic and this enabled GCHR to access global internet data: K. Shubber, A simple guide to GCHR's internet surveillance programme Tempora, Wired, 24 June 2013 <http://www.wired.co.uk/news/archive/2013-06/24/gchq-tempora-101> accessed 14th December 2015; also see O. Bowcott, UK-US surveillance regime was unlawful 'for seven years', The Guardian, 6 February 2015 <http://www.theguardian.com/uk-news/2015/feb/06/gchq-mass-internet-surveillance-unlawful-court-nsa> accessed 1st December 2015

[880] P. Bernal, *Internet Privacy Rights: Rights to Protect Autonomy* (Cambridge, Cambridge University Press 2014) 108

[881] M. Marcovici, *The Surveillance Society: The security vs. privacy debate* (Norderstedt, Books on Demand 2013) 72; GCHQ-NSA intelligence sharing unlawful, says UK surveillance tribunal, Privacy International, 6 February 2015 <https://www.privacyinternational.org/node/482> accessed 1st December 2015

[882] Chris Huhne (2013), 'Prism and Tempora: the cabinet was told nothing of the surveillance state's excesses', The Guardian < https://www.theguardian.com/commentisfree/2013/oct/06/prism-tempora-cabinet-surveillance-state> accessed 25 June 2018.

human rights groups launched a legal challenge following the revelations.[883] The legal challenge argued a violation of the right to private life under Article 8 of the European Convention on Human Rights, raising the question of whether such violation was in accordance with the law. The Uk Investigatory Powers Tribunal considered this question in *Liberty*[884], highlighting that in order for such violation to be deemed to be in accordance with the law, the 'law must indicate the scope of any such discretion conferred on the competent authorities and the manner of its exercise with sufficient clarity to give the individual adequate protection against arbitrary interference'[885]. The ruling was that any interference to private life by the abovementioned systems, as well as other similar systems, was in compliance with the European Convention on Human Rights, acknowledging however that where such arrangements are secret, they will not be sufficiently accessible to the public, noting that such accessibility is key for compliance under the European Convention on Human Rights[886], despite this, it was decided that 'inference of this finding is that the in accordance with the law deficiencies of the surveillance arrangement were remedied by the transparency effectively imposed on the agencies through the pursuit of legal redress'[887].

Moreover, the national security agencies in the UK work together with Europol and other foreign national security agencies and it has been argued that these various agencies require broad preventative powers in order to effectively combat terrorism and

---

[883] Maria Helen Murphy, (2016) 'Transparency and surveillance: assessing the approach of the Investigatory Powers Tribunal in Liberty' Public Law, Jan, 9-18.

[884] *Liberty* [2014] UKIPTrib 13_77-H
[885] *Liberty* [2014] UKIPTrib 13_77-H, 37.
[886] *Liberty* [2014] UKIPTrib 13_77-H.
[887] Maria Helen Murphy, (2016) 'Transparency and surveillance: assessing the approach of the Investigatory Powers Tribunal in Liberty' Public Law, Jan, 9-18

safeguard national security, as well as protect individuals.[888] The terrorist attacks in Paris, Tunisia and other places around the world highlight this and Andrew Parker, the head of M15, explains that it is hardly possible to avert every kind of attack, as terrorist groups employ complicated digital communication methods.[889]

In 1999, the Home Office proposed that an Act should be adopted which permits the interception of communications.[890] The adoption of RIPA was also necessary due to the Human Rights Act 1998 and to achieve compliance with Article of Council Directive 97/66 (the Telecommunications Data Protection Directive).[891] Prior to the enactment of RIPA, a piecemeal approach had been adopted towards the legal control and this posed the threat of litigation in front of the European Court of Human Rights.[892]

Various covert investigation techniques, including intrusive surveillance, were not covered by legislation, which therefore rendered these illegal due to Article 8 of the ECHR.[893] There was no power which permitted the interception of private calls and in *Halford v UK*[894], this was considered to breach Article 8 of the ECHR.[895] Interception of

---

[888] D. Lowe, 'Surveillance and International Terrorism Intelligence Exchange: Balancing the Interests of National Security and Individual Liberty' (2014) *Terrorism and Political Violence*, 1-21, 1

[889] A. Parker, Address by the Director-General of the Security Service to the Royal United Services Institute at Thames House, Security Service MI5, 8th January 2015, 2015 <https://www.mi5.gov.uk/home/about-us/who-we-are/staff-and-management/director-general/speeches-by-the-director-general/director-generals-speech-on-terrorism-technology-and-accountability.html> accessed 1st December 2015; D. Lowe, Why in Widening Surveillance Powers of Electronic Communications, Co-Operation is needed with Internet and Communications Service Providers, Liverpool John Moores University, 1-19, 3

[890] Home Office Consulting Paper, Interception of Communications in the United Kingdom, Cm 4368. 1999; Y. Akdeniz, N. Taylor, C. Walker, 'Regulation of Investigatory Powers Act 2000 (1): Bigbrother.gov.uk: State surveillance in the age of information and rights' (2001) *Criminal Law Review*, 73-90, 74

[891] Y. Akdeniz, N. Taylor, C. Walker, 'Regulation of Investigatory Powers Act 2000 (1): Bigbrother.gov.uk: State surveillance in the age of information and rights' (2001) *Criminal Law Review*, 73-90, 74

[892] Ibid, 75

[893] E.g. see *Kopp v Switzerland* (1999) 27 EHRR 91, at para.74;

[894] *Halford v UK* (1997) 24 EHRR 523

[895] B. Emmerson, A. Ashworth, A. Macdonald, *Human Rights and Criminal Justice* (3rd ed, London, Sweet & Maxwell 2012) 325

communications made on portable telephones in the house, which were transmitted via public networks, was also unlawful following the House of Lords case in *R v Effick*[896] which decided that radio signals which were received on a handset, as opposed to on a base unit, were not part of the public telecommunications system.[897] In light of the increase in crimes facilitated by technology or directed against technology, it was considered that interception plays an essential role in assisting law enforcement agencies.[898] The Interception of Communications Act 1985 therefore became replaced by RIPA.[899]

In *AJA and Others v Metropolitan Commissioner*[900], it was explained that the RIPA provides government agencies with the following covert investigatory powers: Firstly, Part 1 of the Act (s.24(5)(2)) permits that communications are intercepted; Part II permits intrusive surveillance; Part III deals with requests for decryption; Part II contains provisions in respect of Covert Human Intelligence Sources; Part II deals with directed surveillance; and Part 1, Chapter 2 and s.24(5)(2) deal with acquiring meta data i.e. communications data, i.e. about the destinations and origins of phone message, though not their content.[901]

Not as many agencies are allowed to intercept communications, to conduct intrusive surveillance and to demand decryption and stricter requirements are applied i.e. the

[896] *R v Effick* (1995) 1 AC 309
[897] B. Emmerson, A. Ashworth, A. Macdonald, *Human Rights and Criminal Justice* (3rd ed, London, Sweet & Maxwell 2012) 325
[898] Home Office, Interception of Communications in the United Kingdom, Cm 4368, 1999, i
[899] B. Emmerson, A. Ashworth, A. Macdonald, *Human Rights and Criminal Justice* (3rd ed, London, Sweet & Maxwell 2012) 325
[900] *AJA and Others v Metropolitan Commissioner* (2014) 1 All ER 882, per Lord Dyson MR at 8-9
[901] J. Alder, *Constitutional and Administrative Law* (10th ed, London, Palgrave 2015) 569

Secretary of State has to sign in person a warrant or the Secretary of State has to subsequently sign a warrant or a judge or the Surveillance Commissioner has to give prior approval.[902] Only the main investigating bodies can evoke the power to intercept communications i.e. the police, the intelligence services and the Serious Organised Crimes Authority, whereas in respect of intrusive surveillance and decryption additionally, the Armed Forces, the Financial Conduct Authority and the Ministry of Defence are also permitted this, though some exceptions apply in respect of decryption.[903]

A warrant can be granted when national security, the economic well-being of the UK requires this and to prevent and detect serious crime.[904] Those responsible for authorising any of these powers have to consider whether a less intrusive means could be used to gather the information.[905]

In contrast, in respect of CHIS, directed surveillance and the acquisition of meta data it is not necessary that a warrant is obtained or that prior approval has to be sought.[906] Instead various officials, as well as public authorities can authorise this.[907] These powers can be used for public health, public safety and non-serious crime and it is not required to consider whether other less intrusive means could be used.[908]

---

[902] S.24(5)(4) of RIPA; J. Alder, *Constitutional and Administrative Law* (10th ed, London, Palgrave 2015) 569
[903] Ibid (Alder)
[904] S.5 of RIPA
[905] J. Alder, *Constitutional and Administrative Law* (10th ed, London, Palgrave 2015) 569
[906] Ibid
[907] Ibid
[908] Ibid

Part IV of RIPA also creates the Intelligence Services Commissioner, the Investigatory Powers Commissioner for Northern Ireland. and the Interception of Communications Commissioner.[909] S.65 of RIPA established a Regulation of Investigatory Powers Tribunal, which can hear cases where the Human Rights Act 1998 has been violated, or complaints of abuse of powers, or cases of detriments and cases brought against the intelligence services.[910] RIPA thus sets out a governance framework for interception, surveillance, data acquisition and decryption, which is discussed next.

3.2.1 RIPA and Interception

Interception is dealt with in Part I of RIPA. An interception is what is being collected during a transmission.[911] A communication is intercepted by a person if the:

> *contents of the communication [is made] available, while being transmitted, to a person other than the sender or intended recipient of the communication."*[912]

Yet the main term *"content"* has been left undefined, but communications data has been defined, so that data which does not constitute communications data is considered content.[913]

---

[909] S.57(1) of RIPA; B. Emmerson, A. Ashworth, A. Macdonald, *Human Rights and Criminal Justice* (3rd ed, London, Sweet & Maxwell 2012) 333
[910] B. Emmerson, A. Ashworth, A. Macdonald, *Human Rights and Criminal Justice* (3rd ed, London, Sweet & Maxwell 2012) 333
[911] S.1(1) and s.1(2) or RIPA; s.48(1) and (4) of the Wireless Telegraphy Act 2006; D. Anderson, *A Question of Trust* (London, Her Majesty's Stationery Office 2015) 95
[912] S.2(2)(a)-(c) of RIPA; D. Anderson, *A Question Of Trust* (London, Her Majesty's Stationery Office 2015) 95
[913] Anderson (ibid)

S.21(4) of RIPA defines communications data as follows:

> *(a) "any traffic data comprised in or attached to a communication (whether by the sender or otherwise) for the purposes of any postal service or telecommunication system by means of which it is being or may be transmitted;*
>
> *(b) any information which includes none of the contents of a communication (apart from any information falling within paragraph (a)) and is about the use made by any person—*
>
> *(i) of any postal service or telecommunications service; or*
>
> *(ii) in connection with the provision to or use by any person of any telecommunications service, of any part of a telecommunication system;*
>
> *(c) any information not falling within paragraph (a) or (b) that is held or obtained, in relation to persons to whom he provides the service, by a person providing a postal service or telecommunications service."*

Another way to describe communication data is data which identifies the person making the communication; the person receiving the communication; the location where the communication took place; the communication services which were used; and the way in which these services were accessed.[914] Examples of interception may be text messages or emails and this results in the reader being able to see the content, as well as

[914] Communications Data Code, paras2.12-.2.29; s.21(4) of RIPA; C. Harfield, K. Harfield, *Covert Investigation* (3rd ed, Oxford, Oxford University Press 2012) 105

the communications data.[915] A transmission also includes stored data (s.2(7) of RIPA) and this was confirmed by the Court of Appeal in *R v Coulson and another*.[916] As a result, voicemails, which were kept on a phone, can be intercepted. Information which is stored on clouds or on other devices can also be intercepted by virtue of the statutory provisions. [917] Hence, hacking and computer network exploitation (CNE) are permissible.[918]

S.21(4)(c) of RIPA explains that subscriber information is all the information which the service provider holds, as a result of the person signing up to the service. Examples of subscriber information are details about the identity of the person who operates an email account or who can post on a website; installation and billing addresses; or demographic data which was provided. [919] S.21(4)(b) and 22(4) of RIPA define service use information. This consists of itemised call records or internet connections; length and time of service use; details about the data which has been downloaded and uploaded; use of redirection and forward services; and use of special services, such as conference calling.[920]

S.21(4)(a) and s.21(6) of RIPA define traffic data as information which identifies the address, location, person or apparatus of the communication which has been transmitted and the information about the program or file that has been run or accessed whilst

[915] Also see 20 of RIPA; D. Anderson, *A Question Of Trust* (London, Her Majesty's Stationery Office 2015) 95
[916] (2013) EWCA Crim 1026
[917] D. Anderson, *A Question Of Trust* (London, Her Majesty's Stationery Office 2015) 95
[918] Ibid
[919] Paras2.25-2.29 of the Communications Data Code; C. Harfield, K. Harfield, *Covert Investigation* (3rd ed, Oxford, Oxford University Press 2012) 106
[920] also see paras2.23-2.24 of the Communications Data Code; Harfield and Harfield (ibid) 105-106

receiving or sending the communication. An example of traffic data is location data.[921] *"[T]raffic data may identify a server or domain name (web site) but not a web page"*[922], but this creates some confusion since RIPA does not define content.[923] Also, when a service provider stores dynamic IP addresses, then this becomes subscriber information.[924]Traffic data is considered most intrusive, whereas subscriber information is least intrusive and service use information falls in the middle.[925] As a result, particular public authorities can only ask for subscriber and service use information.[926]

Ministers issue warrants, as opposed to courts, though the number of individuals who can apply for a warrant is limited.[927] Furthermore, sections 3-4 explain that for certain kinds of interceptions no warrant is needed, e.g. for prisoners or where the parties have consented to this. Yet when one party only consents and the surveillance is an authorised one under Part II of RIPA, then the stricter warrant criteria in Part I do not have to be discharged, but only the less strict criteria in Part II.[928] This is controversial, as one party may consent that the communication is intercepted, but the other party does not know about this and to then allow that this escapes Part I is questionable.[929] Furthermore, the way interception of telecommunications is defined results in devices on which one can eavesdrop or which result in the content being recorded without

[921] D. Anderson, *A Question Of Trust* (London, Her Majesty's Stationery Office 2015) 96
[922] Para.2.20 of the Acquisition Code
[923] D. Anderson, *A Question Of Trust* (London, Her Majesty's Stationery Office 2015) 96
[924] Ibid
[925] Ibid
[926] Also see The Regulation of Investigatory Powers (Communications Data) Order 2010 (SI 480/2010); D. Anderson, *A Question Of Trust* (London, Her Majesty's Stationery Office 2015) 97
[927] S. Foster, *The Judiciary, Civil Liberties and Human Rights* (Edinburgh, Edinburgh University Press 2006) 141
[928] B. Emmerson, A. Ashworth, A. Macdonald, *Human Rights and Criminal Justice* (3rd ed, London, Sweet & Maxwell 2012) 327
[929] Also see *R v Allsop* (2005) EWCA Crim 703; *R v E* (2004) 1 WLR 2379; B. Emmerson, A. Ashworth, A. Macdonald, *Human Rights and Criminal Justice* (3rd ed, London, Sweet & Maxwell 2012) 327

causing an interference with the transmission signal to fall within Part II and not Part I.[930] This is because for there to be a telecommunications interception, this has to result in a modification or interference with the operation or system, or result in the transmissions being monitored by the system or wireless telegraphy.[931]

Sections 15 and 16 spell out protective safeguards in respect of intercept material.[932] For instance, s.15(4) requires that such material has to be destroyed when there are no longer *"authorised purposes."*[933] Retention of intercept material after a person has been charged may constitute an offence pursuant to s.19 of RIPA and in *R v Preston,*[934] the House of Lords made clear that the purposes for which an intercept authorisation has been granted did not extend to prosecuting offences.[935] Consequently, the objective of ensuring fairness within criminal court proceedings is not a reason to retain intercept material.[936] Para.7.2 of the Interception of Communications Code of Practice[937] explains that it is *"rare"* not to destroy intercept material before a criminal charge is brought.[938] Emmerson states that this makes it more difficult to identify a "*miscarriage of justice"* and this issue is heightened because it is prohibited that intercept material is disclosed, as further discussed below.[939]

[930] S.2(2) of RIPA; Emmerson et al (ibid) 327
[931] Emmerson et al (ibid) 327
[932] Ibid, 328
[933] Ibid
[934] *R v Preston* (1994) 2 AC 130
[935] Emmerson et al (ibid) 328
[936] Ibid
[937] SI 2002/1693 promulgated by virtue of s.71 of RIPA
[938] Emmerson et al (ibid) 328
[939] Ibid

Apart from RIPA, the Wireless Telegraphy Act 2006 also authorises enforcement agencies to intercept data.[940] Under sections 48 and 49 of the Wireless Telegraphy Act 2006, the Commissioners of Revenue and Customs and the Secretary of State can authorise that wireless and other communications are intercepted when one of the statutory purposes applies, including when this is required for national security and to prevent crime.[941] Furthermore, in the High Court case *R (on the application of NTL Group Ltd) v Ipswich Crown Court*[942], it was confirmed that outside the RIPA safeguards, uncontrolled interception can take place. The court found that the police can demand that telecommunications providers intercept emails without a warrant, as required by s.5 of RIPA, but on the basis of broad policing powers conferred by s.9 of the Police and Criminal Evidence Act 1984.[943] This calls into doubt the checks and balances system as set out in RIPA.

3.2.2 RIPA and Surveillance

Part II of RIPA regulates surveillance. S.48(2) of RIPA makes clear that surveillance includes:

> *"(a) monitoring, observing or listening to persons, their movements, their conversations or their other activities or communications;*

[940] Also see the Prison Service Instructions and s.4(4) of RIPA; s.47 of the Prison Act 1952; D. Anderson, *A Question Of Trust* (London, Her Majesty's Stationery Office 2015) 97
[941] Anderson (ibid) 97
[942] (2002) EWHC 1585
[943] Y. Jewkes, M. Yar, *Handbook of Internet Crime* (Abingdon, Routledge 2011) 426

(b) recording anything monitored, observed or listened to in the course of surveillance; and

(c) surveillance by or with the assistance of a surveillance device."

Surveillance results in a pro-active, as opposed to a reactive policing approach, provides high-quality evidence and overcomes the issue that the public is reluctant to furnish information to the police.[944] Yet Klitou highlights that it is important that surveillance is not employed for trivial offences, but rather serious crimes; hence, surveillance should be used to detect or prevent crime or for national security reasons.[945] Yet the problem is that RIPA spells out broad investigatory powers and it is important that these are not abused.[946]

Restrictions are imposed and, for instance, s.26 makes clear that RIPA only applies in case there is intrusive or directed surveillance.[947] Yet Omerod observes that a failure to obtain an authorisation does not constitute an offence. [948]Not all public bodies authorised to conduct directed surveillance are permitted to undertake intrusive surveillance.[949] RIPA defines those public bodies entitled to conduct intrusive surveillance as: any police force, GCHQ, M15 and M16, HM Revenue and Customs, and the Serious Organised Crime Agency.[950] The circumstances allowing for intrusive surveillance are

[944] C. Rogers, R. Lewis, T. John, T. Read, *Police Work: Principles and Practice* (Abingdon, Routledge 2011) 131
[945] D. Klitou, *Privacy-Invading Technologies and Privacy by Design: Safeguarding Privacy, Liberty and Security in the 21st Century* (The Hague, TMC Asser Press 2014) 145-146
[946] Ibid
[947] D. Ormerod, *Blackstone's Criminal Practice 2012* (Oxford, Oxford University Press 2011) 1260
[948] Ibid
[949] C. Harfield, K. Harfield, *Covert Investigation* (3rd ed, Oxford, Oxford University Press 2012) 54
[950] S.32(6) and s.41(1) of RIPA; Harfield and Harfield (ibid) 54-55

more limited than that of directed surveillance.[951]Whilst the circumstances which are covered by RIPA is expansive, it only relates to surveillance in the UK, [952]and it must comply with the ECHR.[953]Pursuant to the Police Act 1997 and s.71 of RIPA, codes of practices are published, which have to be followed in order to ensure that an authorised interference is lawful.[954] The Interception of Communications Commissioner and the Chief Surveillance Commissioner are entrusted with overseeing RIPA.

Directed surveillance denotes less intrusion than intrusive surveillance; it requires authorisation and the threshold is crime, whereas for intrusive surveillance the threshold is serious crime.[955] The Protection of Freedoms Act 2012 amends RIPA and thereby ensures that the power of public authorities to conduct surveillance is further curtailed.[956] In the context of cybercrime, it may be useful to clarify which offences should be considered serious. Furthermore, s.28(3) of RIPA explains that an authorisation for directed surveillance can be granted when it is considered necessary:

> *"(a) in the interests of national security;*

[951] Harfield and Harfield (ibid) 54
[952] D. Lowe, 'Surveillance and International Terrorism Intelligence Exchange: Balancing the Interests of National Security and Individual Liberty' (2014) *Terrorism and Political Violence*, 1-21, 3
[953] Ibid; Home Office, Regulation of Investigatory Powers Act 2000 guidance, 18 December 2013, 1-19, 4 <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/453708/ripa1.pdf> accessed 1st December 2015
[954] C. Rogers, R. Lewis, T. John, T. Read, *Police Work: Principles and Practice* (Abingdon, Routledge 2011) 132
[955] S.28(3), s.81(2) and s.81(5) of RIPA; C. Harfield, *Blackstone's Police Operational Handbook: Practice and Procedure* (Oxford, Oxford University Press 2009) 101
[956] P. Coppel, *Information Rights: Law and Practice* (Oxford, Hart Publishing 2014) 577

(b) for the purpose of preventing or detecting crime or of preventing disorder;

(c) in the interests of the economic well-being of the United Kingdom;

(d) in the interests of public safety;

(e) for the purpose of protecting public health;

(f) for the purpose of assessing or collecting any tax, duty, levy or other imposition, contribution or charge payable to a government department; or

(g) for any purpose (not falling within paragraphs (a) to (f)) which is specified for the purposes of this subsection by an order made by the Secretary of State."

Harfield further explains that in relation to agencies other than the police, these statutory purposes are limited to particular agencies.[957] Statutory instruments have been enacted to detail which particular agency can use directed surveillance for which particular purposes.[958]

As mentioned, for intrusive surveillance to be authorised, a higher threshold of crime has to be present. Authorisation is therefore stricter, also because necessity, as well as proportionality have to be established and it is mandated to consider whether other means could reasonably be used.[959] S.81(2)(b) and s.81(3) of RIPA define serious crime as:

[957] C. Harfield, *Blackstone's Police Operational Handbook: Practice and Procedure* (Oxford, Oxford University Press 2009) 101
[958] Ibid
[959] B. Emmerson, A. Ashworth, A. Macdonald, *Human Rights and Criminal Justice* (3rd ed, London, Sweet & Maxwell 2012) 331

"(a) that the offence or one of the offences that is or would be constituted by the conduct is an offence for which a person who has attained the age of twenty-one and has no previous convictions could reasonably be expected to be sentenced to imprisonment for a term of three years or more;

(c) that the conduct involves the use of violence, results in substantial financial gain or is conduct by a large number of persons in pursuit of a common purpose."

S.26(2) of RIPA defines intrusive surveillance as:

"covert surveillance that

(a) is carried out in relation to anything taking place on any residential premises or in any private vehicle; and

(b) involves the presence of an individual on the premises or in the vehicle or is carried out by means of a surveillance device."

When intrusive surveillance has been authorised, the Surveillance Commissioner has to be informed, who has to then approve this.[960] Apart from RIPA, the Digital Economy Act 2010 also implicitly permits surveillance to enforce copyright.[961]

[960] S.35 of RIPA
[961] W. Merrin, *Media Studies 2.0* (Abingdon, Routledge 2014) 159

3.2.3 RIPA and Decryption

When encrypted content is intercepted, then it cannot be used.[962] Equally, when an encrypted device is legally seized, then it is important that enforcement officers have the power to demand that the key to decrypt the device is provided.[963] This power was activated in 2007, but despite being extremely intrusive, it is not covert.[964] S.49(2) of RIPA permits certain individuals, as defined in Schedule 2, to send a Part 3 notice to those persons, who can be reasonably considered to possess the encryption key, so that they can disclose it.[965] However, a written permission has to be obtained from a Circuit Judge or a District Judge (Magistrates' Courts)[966] or a warrant has to be issued.[967] However, the intelligence services do not have to ask for a warrant, but have the power to do this by virtue of statute.[968] Some other exceptions apply, for instance, to the police, the Serious Organised Crime Agency (SOCA) and the Scottish Crime and Drug Enforcement Agency (SCEDEA), so that no warrant has to be sought, but this power arises by virtue of statute.[969] Accordingly, enforcement agencies can request secret decryption passwords or keys or can require persons to decrypt message, so long as the Secretary of State, senior officials or circuit judges have authorised this.[970] Those required to provide the key are frequently required to provide a secrecy undertaking, so

[962] Y. Jewkes, M. Yar, *Handbook of Internet Crime* (Abingdon, Routledge 2011) 426
[963] S.49 of RIPA; D. Anderson, *A Question Of Trust* (London, Her Majesty's Stationery Office 2015) 146
[964] Anderson (ibid) 146
[965] Y. Jewkes, M. Yar, *Handbook of Internet Crime* (Abingdon, Routledge 2011) 426
[966] Schedule 2, Article 1(1)(a) of RIPA
[967] Schedule 2, Article 2 of RIPA
[968] Schedule 2, Article 3 of RIPA
[969] Schedule 2, Article 4 of RIPA
[970] B. J. Goold, D. Neyland, *New Directions in Surveillance and Privacy* (Cullompton, Willan Publishing 2009) 50

that they cannot discuss this with anyone, apart from their legal adviser.[971] A failure to comply with a notice can result in an imprisonment for up to two years and up to five years in respect of matters which relate to national security[972] and for not complying with the secrecy requirement.[973] Hence, a *"tipping off"* offence has been created, which can be committed by those receiving a notice.[974]

Third parties who provide encryption services, may frequently receive such notices.[975] For instance, internet service providers, which offer secure IP telephony services or virtual private network may be requested to make available the particular decryption keys or unencrypted data traffic.[976] When a digital investigation is carried out, various ways are used to access encrypted evidence, for instance, the suspect can be forced or persuaded to furnish the decryption key; passphrases or keys can be located; unencrypted copies of the data may be located; a smart password attack can be conducted; implementation vulnerabilities can be exploited, software and hardware surveillance can be conducted; or an exhaustive key search may be undertaken.[977] From a technological perspective, it is also possible for enforcement agents to launch a *"man-in-the-middle"* attack in respect of encrypted communications and to thereby obtain information.[978] Service providers, such as Skype, could also be requested to use weak

---

[971] Ibid
[972] Also see s.15 of the Terrorism Act 2006
[973] B. J. Goold, D. Neyland, *New Directions in Surveillance and Privacy* (Cullompton, Willan Publishing 2009) 50
[974] Ss53-54 of RIPA; B. Emmerson, A. Ashworth, A. Macdonald, *Human Rights and Criminal Justice* (3rd ed, London, Sweet & Maxwell 2012) 332
[975] B. J. Goold, D. Neyland, *New Directions in Surveillance and Privacy* (Cullompton, Willan Publishing 2009) 50
[976] Ibid
[977] C. Hargreaves, H. Chivers, 'Detecting Hidden Encrypted Volumes' in (eds) B. De Decker, I. Schaumüller-Bichl, *Communications and Multimedia Security: 11th IFIP TC 6/TC 11 International Conference, CMS 2010, Linz, Austria, Ma/June 2010, Proceedings* (New York, Springer 2010) 234
[978] B. J. Goold, D. Neyland, *New Directions in Surveillance and Privacy* (Cullompton, Willan Publishing 2009) 50

encryption in respect of a particular target.[979] Yet Goold and Neyland states that such co-operation does not yet take place.[980]

3.4 Data Retention: The EU Data Retention Directive, the UK Data Retention and Investigatory Powers Act 2014 and the Investigatory Powers Act 2016

Governments are interested in creating a *"digital mass surveillance framework"*, which collects, retains and processes data about all the interactions, transactions and uses of communication and information technologies.[981] The European Commission reports that evidence from Europol and the Member States highlights the importance of retaining communications data for criminal investigations and prosecutions.[982] Mandatory data retention ensures that valuable data is accessible for a certain time period. Operators may otherwise not store data in an easy to retrieve manner or at all, as they have no real business value.[983] This type of data includes, for instance, unsuccessful phone calls; IP addresses; or email data.[984] Without the storage of particular traffic data, it becomes virtually impossible to investigate and detect certain crimes. For instance, the German federal police reported that for nearly half of cases, they could not have conducted an

[979] Ibid
[980] Ibid
[981] A. A. Casilli, Four These on Digital Mass Surveillance and the Negotiation of Privacy, 8th Annual Privacy Law Scholar Congress 2015, Jun 2015, Berkeley, United States, 2015, 1-14, 1 <https://halshs.archives-ouvertes.fr/halshs-01147832/document> accessed 1st December 2015
[982] European Commission, Evidence for necessity of data retention in the EU, March 2013, 1-29, 1 <http://ec.europa.eu/dgs/home-affairs/pdf/policies/police_cooperation/evidence_en.pdf> accessed 15th December 2015
[983] Ibid, 5
[984] Ibid, 5

investigation without being able to access the historical traffic data.[985] The terrorist attacks in London and Madrid in 2004/2005 particularly highlighted the importance and the EU therefore adopted a Framework Decision on Police and Judicial Cooperation in Criminal Matters.[986] As the law was not harmonised in the Member States, in 2006 the Data Retention Directive (2006/24/EC) was enacted.[987]

Providers of public communications networks and electronic communications services were required to keep data, so that the destination and source of fixed mobile and internet telephony and network, emails, text messages and internet access could be identified.[988] The Directive required that internet and telephone traffic was to be retained for 6 months and up to two years, so that terrorism and organised crime could be combated.[989] User names, numbers, time, date and duration, the international mobile subscriber identity and international mobile station equipment identity for mobile phones, including the place of the cell ID, had to be retained.[990] Hence, in Europe telephone companies had to retain data about each mobile and land line call and other details, whilst internet service providers had to keep data about internet connections and

[985] Sachstandsbericht Nr. 8: Stand der statistischen Datenerhebung im BKA, 23 June 2011, 13; European Commission, Evidence for necessity of data retention in the EU, March 2013, 1-29, 6 <http://ec.europa.eu/dgs/home-affairs/pdf/policies/police_cooperation/evidence_en.pdf> accessed 15th December 2015
[986] F. Bieker, 'The Court of Justice of the European Union, Data Retention and the Rights to Data Protection and Privacy - Where Are We Now?' in (eds) J. Camenisch, S. Fischer-Hübner, M. Hansen, *Privacy and Identity Management for the Future Internet in the Age of Globalisation* (London, Springer 2015) 74
[987] Ibid
[988] Article 5(1) of the Data Retention Directive;
[989] C. R. Martin, S. L. Weakley, *Internet Law and Practice in California* (Oakland, CEB 2015) para.21.18A
[990] F. Bieker, 'The Court of Justice of the European Union, Data Retention and the Rights to Data Protection and Privacy - Where Are We Now?' in (eds) J. Camenisch, S. Fischer-Hübner, M. Hansen, *Privacy and Identity Management for the Future Internet in the Age of Globalisation* (London, Springer 2015) 74

addresses, as well as details to trace emails and voice over internet protocol (VoIP) calls.[991] Yet Article 5(2) of the Data Retention Directive proscribed the storage of data which showed the contents.[992]

In 2012, the Irish High Court and the Australian Constitutional Court made a preliminary reference to the CJEU in order to ask whether the Data Retention Directive was compatible with fundamental rights.[993] Granger and Irion comment that thereby the controversial *"Big Brother policies"* were challenged.[994] The issue was whether data retention had to be analysed against the background of the right to privacy as guaranteed in Article 7 of the Charter of Fundamental Rights (CFR) and the right to protection of personal data as guaranteed in Article 8 of the CFR and as a result imposed requirements on data retention.[995] For instance, Article 8 expressly provides that personal data *"[m]ust be processed fairly for specified purposes and on the basis of the consent of the person concerned or other legitimate basis laid down by law ..."* and that an *"independent authority"* has to monitor to guarantee this right.[996] The constitutional principles contained in Articles 7 and 8 were firstly introduced through Directive 95/46

[991] C. R. Martin, S. L. Weakley, *Internet Law and Practice in California* (Oakland, CEB 2015) para.21.18A
[992] F. Bieker, 'The Court of Justice of the European Union, Data Retention and the Rights to Data Protection and Privacy - Where Are We Now?' in (eds) J. Camenisch, S. Fischer-Hübner, M. Hansen, *Privacy and Identity Management for the Future Internet in the Age of Globalisation* (London, Springer 2015) 74
[993] Ibid, 75
[994] M.-P. Granger, K. Irion, 'The Court of Justice and the Data Retention Directive in Digital Rights Ireland: Telling Off the EU Legislator and Teaching a Lesson in Privacy and Data Protection' (2014) 6 *European Law Review*, 835-850, 837
[995] F. Bieker, 'The Court of Justice of the European Union, Data Retention and the Rights to Data Protection and Privacy - Where Are We Now?' in (eds) J. Camenisch, S. Fischer-Hübner, M. Hansen, *Privacy and Identity Management for the Future Internet in the Age of Globalisation* (London, Springer 2015) 75
[996] M.-P. Granger, K. Irion, 'The Court of Justice and the Data Retention Directive in Digital Rights Ireland: Telling Off the EU Legislator and Teaching a Lesson in Privacy and Data Protection' (2014) 6 *European Law Review*, 835-850, 837

on the protection of individuals with regard to processing of personal data and on the free movement of such data (the Data Protection Directive) and Directive 2002/59 concerning the processing of personal data and the protection of privacy in the electronic communications sector (ePrivacy Directive).[997] The ePrivacy Directive states that electronic communications, as well as traffic data has to be kept confidential, though Article 15(1) permits Member States to retain data for a limited time, so long as these are *"necessary, appropriate and proportionate measures within a democratic society to safeguard national security i.e. State security, defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system, as referred to in Article 13(1) of Directive 95/46/EC."*[998]

Advocate General Cruz Villalon argued that the Directive should be declared invalid since it contravenes Article 7.[999] He suggested that it should firstly be assessed whether the Directive is proportionate in relation to the general means employed and the measure which is meant to be achieved in accordance with Article 5(4) of the TEU; and, secondly, it should be analysed whether it complies with the Charter, particularly the proportionality provision in Article 52(1) of the Charter of Fundamental Rights.[1000] He considered that the degree of interference with fundamental rights was substantively disproportionate.[1001] He evaluated whether the interference was permitted by law,

[997] Ibid
[998] P. Bernal, *Internet Privacy Rights: Rights to Protect Autonomy* (Cambridge, Cambridge University Press 2014) 95; S. Gutwirth, R. Leenes, P. de Hert, Y. Poullet, *European Data Protection: Coming of Age* (Cambridge, Cambridge University Press 2014) 71
[999] Opinion of A.G. Cruz Villalon in *Digital Rights Ireland* (C-293/12) (2013) ECR I-845
[1000] Ibid, 1
[1001] Ibid, 102

guaranteed the right to privacy, was not disproportionate i.e. was necessary and meeting legitimate objectives. He criticised the EU legislator and stated that *"[t]he EU legislature [could] not when adopting an act imposing obligations which constitutes serious interference with the fundamental rights of citizens of the Union, entirely leave to the Member States the task of defining the guarantees capable of justifying that interference … It must … fully assume its share of responsibility…"*[1002]

In 2014, the Grand Chamber of the CJEU then issued its judgment in the *Digital Rights Ireland* case.[1003] It found that the Directive impacted the right to freedom of expression and violated privacy rights in a disproportionate manner, which did not serve the public interest to ensure safety.[1004] The court emphasised that too much insight was gained about the life of all normal citizens, despite the fact that no content was stored.[1005] The court stated that the effect of the Directive was that persons felt that their entire private lives were constantly under surveillance.[1006]

It found that the data retention requirement and affording national authorities access amounted to interferences. National authorities could use and access the data without any limitation being imposed, as they could define what constitutes serious crime, as

[1002] Ibid, 120; M.-P. Granger, K. Irion, 'The Court of Justice and the Data Retention Directive in Digital Rights Ireland: Telling Off the EU Legislator and Teaching a Lesson in Privacy and Data Protection' (2014) 6 *European Law Review*, 835-850, 840-841
[1003] Joined Cases C/293/12 and C-594/12 *Digital Rights Ireland and Seitlinger and others*
[1004] C. R. Martin, S. L. Weakley, *Internet Law and Practice in California* (Oakland, CEB 2015) para.21.18A
[1005] Joined Cases C/293/12 and C-594/12 *Digital Rights Ireland and Seitlinger and others*, at 27
[1006] Ibid, at 37

well as the procedural and substantive conditions.[1007]Articles 7 and 8 of the EU Charter of Fundamental Rights were breached by the fact that data had to be retained for two years.[1008] It was made clear that the Data Retention Directive is a derogation from the Directive on privacy and electronic communications (2002/58/EC).[1009] Article 1(3) of the Directive on privacy and electronic communications contains an exception for judicial and police cooperation. The almost identical exception is found in Article 3(2) of the Data Protection Directive 95/46/EC. Nonetheless, the CJEU acknowledged that data retention is a suitable measure to combat serious crime and international terrorism, but made clear that this is subject to strict requirements, so that Article 8 (the right to privacy) and fundamental rights are safeguarded.[1010] It also confirmed that use of modern investigation methods was important to combat terrorism and organised crime.[1011]

The court stressed that legislation which interferes with rights must spell out precise and clear rules, so that the scope of the measure and its application is defined and minimum safeguards are imposed, so that persons are afforded with adequate guarantees to protect

[1007] F. Bieker, 'The Court of Justice of the European Union, Data Retention and the Rights to Data Protection and Privacy - Where Are We Now?' in (eds) J. Camenisch, S. Fischer-Hübner, M. Hansen, *Privacy and Identity Management for the Future Internet in the Age of Globalisation* (London, Springer 2015) 77

[1008] A. Roberts, Privacy, Data Retention and Domination: Digital Rights Ireland Ltd v Minister for Communications, 78(3) *Modern Law Review* 2015, 535-548, 535

[1009] F. Bieker, 'The Court of Justice of the European Union, Data Retention and the Rights to Data Protection and Privacy - Where Are We Now?' in (eds) J. Camenisch, S. Fischer-Hübner, M. Hansen, *Privacy and Identity Management for the Future Internet in the Age of Globalisation* (London, Springer 2015) 82

[1010] Joined Cases C/293/12 and C-594/12 *Digital Rights Ireland and Seitlinger and others*, 41- 44 and 49; J. Kuhling, S. Heitzer, Returning through the National Back Door? The future of data retention after the ECJ Judgment on Directive 2006/24 in the UK and Elsewhere, 2 *European Law Review* 2015, 263-278, 263

[1011] Joined Cases C/293/12 and C-594/12 *Digital Rights Ireland and Seitlinger and others*, at 51

their data effectively against unlawful access, use and abuse of the data.[1012] Firstly, there was no link with the retention of the communications data and particular security threats and professional secrecy was thereby also not protected.[1013] Secondly, no limits were imposed and no objective criteria were developed in respect of access and use and there were no procedural and substantive conditions, despite it being crucial to strictly limit the purpose when averting and detecting particular serious offences or those necessary to pursue a criminal prosecution.[1014] Hence, it is crucial that serious crime is defined and objective requirements are adopted, so that only certain persons are permitted to access and use the data when this is absolutely necessary.[1015] Accordingly, a *"blanket retention of traffic data"* to combat terrorism and crime is not allowed.[1016] Hence, a *"strict scrutiny test"* has been adopted and it has to be strictly assessed whether the measures are proportionate and necessary when there is a serious interference with fundamental rights, even when legitimate objectives are pursued.[1017] Following the decision, domestic law makers have to develop a governance system, which has the necessary *"checks and balances."*[1018] Consequently, data collection should be limited to situations where there exists a risk to public security; hence, should take place only for a certain time period, be restricted to a geographical area or a particular group of individuals.[1019]

[1012] Ibid, at 54
[1013] Ibid, at 58
[1014] Ibid, at 61
[1015] Ibid, at 60&62
[1016] F. Bieker, 'The Court of Justice of the European Union, Data Retention and the Rights to Data Protection and Privacy - Where Are We Now?' in (eds) J. Camenisch, S. Fischer-Hübner, M. Hansen, *Privacy and Identity Management for the Future Internet in the Age of Globalisation* (London, Springer 2015) 72
[1017] Council of the European Union, General Secretariat, Judgment of the Court of 8 April 2014 in joined Cases C-293/12 and C-594/12, 5 May, 2014, 909/14 JUR; M.-P. Granger, K. Irion, 'The Court of Justice and the Data Retention Directive in Digital Rights Ireland: Telling Off the EU Legislator and Teaching a Lesson in Privacy and Data Protection' (2014) 6 *European Law Review*, 835-850, 845
[1018] Granger and Irion (ibid), 848
[1019] *Digital Rights Ireland* (C-293/12) (2013) ECR I-845, at 59

Data retention has to be supervised by an independent authority, so that personal data is protected and secured.[1020] When retained data is retroactively accessed and used, this should only be done when this is absolutely necessary and in accordance with procedural, as well as substantive conditions.[1021] This means that the purpose has to be limited to serious offences and access requests should be approved by an independent body and only a few persons should be able to access and make use of the data.[1022]

Member States can thus enact legislation, so long as these criteria are satisfied.[1023] This is particularly important due to the increase in terrorism, which puts to the fore the question what substitute should be adopted, so that law enforcement agencies can retain data. [1024] The UK enacted emergency legislation in the form of the Data Retention and Investigatory Powers Act 2014, which permitted police to access the communications of companies, so that they could monitor internet activity and listen to phone records. [1025] The Act was adopted due to the Grand Chamber of the Court of Justice ruling that the EU Data Retention Directive is invalid and as the UK Regulations were based on this, this resulted in a legal gap.[1026] The case illustrates that the surveillance powers which

[1020] Article 29 of the Data Protection Working Party (WP29), Statement on the ruling of the Court of Justice of the European Union which invalidates the Data Retention Directive (2014) 14/EN WP 220; Granger and Irion (ibid) 848
[1021] Granger and Irion (ibid) 849
[1022] Ibid
[1023] J. Kuhling, S. Heitzer, Returning through the National Back Door? The future of data retention after the ECJ Judgment on Directive 2006/24 in the UK and Elsewhere, 2 *European Law Review* 2015, 263-278, 263
[1024] C. R. Martin, S. L. Weakley, *Internet Law and Practice in California* (Oakland, CEB 2015) para.21.18A
[1025] Ibid, para.21.18A
[1026] D. Anderson, *A Question Of Trust* (London, Her Majesty's Stationery Office 2015) 15-16

governments increasingly seek is difficult to reconcile with what courts consider proportionate and necessary.[1027]

The Data Retention and Investigatory Powers Act 2014 (DRIPA 2014) was thus adopted, temporarily, as it was provided for it to be applicable until 31 December 2016, and it has since then been repealed, to ensure that authorisations, warrants and conditions imposed in respect of communications data and interception have extraterritorial effect, so that overseas service providers could also be required to comply.[1028]

Hence, the main aim was to enable security services to request public telecommunications operators to keep communications data in accordance with RIPA.[1029] A report had to be published on an annual basis, in which it was disclosed how much data had been intercepted, and a body had to be created to act as a watchdog to ensure that the powers were not abused.[1030] Not as many public bodies were allowed to collect data and only relevant data could be accessed. Data retention was shortened to twelve months.[1031] A diplomat was also appointed, who was responsible for negotiating data transfers with the US. [1032] S.8 provided that the provisions were only in force until late 2016. The Act became then replaced by the Investigatory Powers Act 2016.[1033]

[1027] R. MacKinnon, E. Hickok, A. Bar, H-I. Lim, *Fostering freedom online: the role of Internet intermediaries* (Paris, UNESCO 2015) 39
[1028] D. Anderson, *A Question Of Trust* (London, Her Majesty's Stationery Office 2015) 16
[1029] L. Scaife, *Handbook of Social Media and the Law* (Abingdon, Routledge 2015) 18
[1030] Ibid
[1031] Ibid
[1032] Ibid
[1033] Hansard, HC Debs 15 July 2014, Col 714 (Theresay May) and Co 723 (Yvette Cooper); D. Anderson, *A Question Of Trust* (London, Her Majesty's Stationery Office 2015) 16; L. Cropper, The Investigatory Powers Act 2016 - A "Snoopers' Charter" or a legitimate surveillance tool for today's society, Field Fisher

In 2012, the UK government announced the Draft Communications Data Bill, but this was criticised as being a *"snooper's charter"* and was not enacted.[1034] Electronic communications services providers would have had to collect more data and make this available to law enforcement agencies and public authorities.[1035] Part 3 of the proposed Bill would have amended the Data Retention and Investigatory Powers Act 2014, so that relevant authorities could identify the device which used the Internet Protocol at a particular time or could identify the person.[1036]

In November 2015, the Draft Investigatory Powers Bill was presented to parliament, which received royal assent in November 2016 and became adopted as the Investigatory Powers Act 2016.[1037] Travis labels this a *"snooper's charter"* since it permits the security services to bug and hack and requires that the personal data of everyone is stored for one year, including the way the web and social and phone media is used.[1038] Furthermore, private and public datasets can be accessed by the Security and

---

LLP, 2 April 2017 <http://privacylawblog.fieldfisher.com/2017/the-investigatory-powers-act-2016-a-snoopers-charter-or-a-legitimate-surveillance-tool-for-todays-society/> accessed 1st December 2017

[1034] J. Castro-Edwards, What the 'snoopers charter' means for business and the public, Guardian, 27 May 2015 <http://www.theguardian.com/media-network/2015/may/27/snoopers-charter-business-public-communications-data> accessed 15th December 2015

[1035] Ibid

[1036] House of Lords, House of Commons, Joint Committee on Human Rights, Legislative Scrutiny: Counter-Terrorism and Security Bill, Fifth Report of Session 2014-15 (London, The Stationery Office Ltd 2015) 22

[1037] A. Travis, 'Snooper's charter' bill becomes law, extending UK state surveillance, The Guardian, 29 November 2016 <https://www.theguardian.com/world/2016/nov/29/snoopers-charter-bill-becomes-law-extending-uk-state-surveillance> accessed 1st December 2017

[1038] A. Travis, Investigatory powers bill: snooper's charter to remain firmly in place, The Guardian, 2 November 2015 <http://www.theguardian.com/world/2015/nov/02/investigatory-powers-bill-snoopers-charter-will-remain-firmly-in-place> accessed 1st December 2015

Intelligence Agencies (SIAs).[1039] Also, the intelligence services can create and analyse *"Bulk Personal Datasets"* and this provides them with intelligence about national security risks and helps with combating crime and protecting the economic well-being.[1040] This ensures that what was disclosed by Edward Snowden is legalised.[1041] The Act states that data shall only be stored for a limited time, except when it is likely that it may be useful at a future date, but since the analysis of data is speculative, the risk is that this may result in a subjective determination.[1042]

Lysnkey highlights that the issue is that individuals may be singled out because they have certain characteristics or are part of a group or have certain interests, which render them suspects.[1043] This may have an impact on them without them knowing or consenting to the processing of their personal data.[1044]However, no content can be collected by phone and internet companies, though a ministerial intercept warrant can authorise the collection of content.[1045] Yet Murray and Keenan point out that this warrant issuing procedure is not overseen by an independent judiciary.[1046] Instead, the

[1039] O. Lysnkey, Beyond privacy: the data protection implications of the IP Bill, Policy Briefing 15, 2015, 1-4, 2 <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2704299> accessed 1st December 2015
[1040] B. Keenan, Bulk data in the draft Investigatory Powers Bill: the challenge of effective oversight, LSE Law Policy Briefing Series 13, 2015, 1-4, 1 <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2703839> accessed 1st December 2015
[1041] A. Travis, Investigatory powers bill: snooper's charter to remain firmly in place, The Guardian, 2 November 2015 <http://www.theguardian.com/world/2015/nov/02/investigatory-powers-bill-snoopers-charter-will-remain-firmly-in-place> accessed 1st December 2015
[1042] B. Keenan, Bulk data in the draft Investigatory Powers Bill: the challenge of effective oversight, LSE Law Policy Briefing Series 13, 2015, 1-4, 3 <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2703839> accessed 1st December 2015
[1043] O. Lysnkey, Beyond privacy: the data protection implications of the IP Bill, Policy Briefing 15, 2015, 1-4, 2-3 <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2704299> accessed 1st December 2015
[1044] Ibid
[1045] A. Travis, Investigatory powers bill: the key points, The Guardian, 4 November 2015 <http://www.theguardian.com/world/2015/nov/04/investigatory-powers-bill-the-key-points> accessed 1st December 2015
[1046] A. Murray, B. Keenan, Ensuring the Rule of Law, LSE Law Policy Briefing Series 12, 2015, 1-4, 3 <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2703806> accessed 1st December 2015

Secretary of State can grant a warrant whenever this is "necessary in the interests of national security"[1047] "or for the purpose of preventing or detecting serious crime" or "in the interests of the economic well-being of the United Kingdom so far as those interests are also relevant to the interests of national security."[1048] Murray and Keenan question whether this may result in *"rubber-stamping"* of the Home Secretary's decisions. It is also noteworthy that internet and phone companies receive a payment from the Home Office for the retention of the data and to give access to the police and security services.[1049]

This investigatory legislation has faced severe backlash from a number of journalists and human rights organisations, including the Bureau of Investigative Journalism, Amnesty International, Privacy International, Big Brother Watch, the Open Rights Group, and the Irish Council for Civil Liberties who in an unprecedented move have filed legal complaints against the UK government with the European Court of Human Rights (ECHR) to challenge the legality of its mass surveillance.[1050] The landmark case was heard on 7 November 2017, when the UK government was accused of violating the right to privacy, the right to a fair trial, the right to freedom of expression, and the right not to be discriminated against, which are all protected under the ECHR convention. Nine judges posed questions to the UK government related to what safeguards are in

[1047] S.138(1)(b)(i) of the Investigatory Powers Act 2016
[1048] S.138(1)(b)(ii) and s.138(2)(a)-(b) of the Investigatory Powers Act 2016
[1049] A. Travis, Investigatory powers bill: the key points, The Guardian, 4 November 2015 <http://www.theguardian.com/world/2015/nov/04/investigatory-powers-bill-the-key-points> accessed 1st December 2015
[1050] R. Gallagher, 'European court to decide whether U.K. mass surveillance revealed by Snowden violates human rights', *The Intercept*, 7 November 2017 <https://theintercept.com/2017/11/07/uk-surveillance-case-european-court-human-rights/> accessed December 2017

place, who controls interception, how easily are warrants granted for communication interception, and on what basis is information selected for human analysis.[1051] A judgement is expected early 2018 and will have major implications for the Investigatory Powers Act, 2016.

3.5 Admissibility of Intercepted Communication in Court Proceedings

In the past, government secrets could be withheld by claiming *"Crown privilege"* and nowadays this is called *"public interest immunity."*[1052] Normally relevant documents have to be disclosed to the other side in court proceedings, but when public interest immunity is successfully pleaded, information does not have to be disclosed.[1053] Hence, whilst the Crown Prosecution Service normally has to disclose all material which weaken the prosecution's case, this is not the case in respect of sensitive material i.e. material which if disclosed harms the public interest.[1054] For instance, a disclosure may reveal particular techniques, which may be used in the future and may therefore not be disclosed.[1055] Disclosure can be prevented by virtue of the public interest common law rules and s.21(2) of the Criminal Procedure and Investigations Act 1996.[1056] Under s.3(6) and s.7(5) of the Criminal Procedure and Investigations Act 1996 an application

[1051] R. Hill, UK's surveillance regime challenged in landmark European court hearing, *The Register*, 7 November 2017 <https://www.theregister.co.uk/2017/11/07/ukgovs_mass_surveillance_regime_grilled_in_landmark_hearing_in_european_court/> accessed December 2017
[1052] C. Forsyth, 'Public Interest Immunity: Recent and Future Developments' (1997) 1 *Cambridge Law Journal*, 51-59, 51
[1053] *Al Rawi v Secretary of State for the Home Department* (2011) UKSC 34; R. Glover, *Murphy on Evidence* (14th ed, Oxford, Oxford University Press 2015) 510
[1054] H. Fenwick, *Civil Liberties and Human Rights* (4th ed, Abingdon, Routledge 2007) 1075
[1055] Ibid
[1056] Ibid

for public interest immunity can be made by the prosecutor to the court, so that material is protected.[1057] This ensures that intercepted communications are only used for investigative purposes.[1058]

However, public interest immunity contravenes the notion of *"open justice"* and therefore raises questions in respect of the right to a fair hearing and also in respect of freedom of expression.[1059] Since the case of *Conway v Rimmer,*[1060] the courts therefore balance whether confidentiality is in the public interest and do not simply accept the request by the enforcement agencies.[1061] Courts can thus inspect documents, which are affected by a public interest immunity claim and then decide whether disclosure should be ordered.[1062]

Once a public interest immunity has been issued, a person, who wants access to a document, can nonetheless challenge the decision to uphold public interest immunity.[1063] He has to demonstrate to the court that this is necessary to provide him with a fair hearing or in a criminal case assists with the defence.[1064] Whilst the court can scrutinise the documents, it is inclined to do this in order to prevent "*speculative fishing*

[1057] Ibid
[1058] C. Rogers, R. Lewis, T. John, T. Read, *Police Work: Principles and Practice* (Abingdon, Routledge 2011) 132
[1059] J. Alder, *Constitutional and Administrative Law* (10th ed, London, Palgrave 2015) 561
[1060] (1968) AC 910
[1061] A. Choo, *Evidence* (3rd ed, Oxford, Oxford University Press 2012) 204
[1062] Ibid
[1063] *Goodridge v Chief Constable of Hampshire Constabulary* (1999) 1 All ER 896; *Air Canada v Secretary of State for Trade (No.2)* (1983) 2 AC 394; s.3 of the Criminal Procedure and Investigations Act 1996; J. Alder, *Constitutional and Administrative Law* (10th ed, London, Palgrave 2015) 562
[1064] *Goodridge v Chief Constable of Hampshire Constabulary* (1999) 1 All ER 896; *Air Canada v Secretary of State for Trade (No.2)* (1983) 2 AC 394; s.3 of the Criminal Procedure and Investigations Act 1996; Alder (ibid) 562

expeditions."[1065] Covert surveillance operations, national security and safeguarding anonymous informers have been found to constitute reasons to reject disclosure applications.[1066] Similarly, commercially or financially sensitive information, for instance, between the Bank of England and the government or with private businesses or communications between the government and foreign governments are also reasons to refuse disclosure.[1067]

In line with the public interest immunity principle, s.17 of RIPA makes clear that intercepted communications are not permitted during court proceedings, which is important for the secret and security intelligence agencies whose work could otherwise be affected.[1068] However, the prohibition to disclose intercept material in s.17 is extremely controversial because it results in a wide range of important material being excluded.[1069] S.17 replicates the principle, which was previously set out in s.9 of the Interception of Communications Act 1985.[1070] Under this principle, no questions can be asked, no evidence can be provided, no disclosure or assertion can be made or any other things in relation or because of the legal proceedings which would reveal that a warrant application was made or that a public official has committed an offence.[1071] However, certain exceptions exist, for instance, intercept material which comes from foreign

[1065] Also see *Burmah Oil Co Ltd v Bank of England* (1980) AC 1090, per Lord Keith at 1136; cited from J. M. Evans, 'Civil Litigation - Discovery - Public Interest Immunity and State Papers' (1980) 58(2) *Canadian Bar Review* 360-376, 375; A. Keane, P. McKeown, *The Modern Law of Evidence* (10th ed, Oxford, Oxford University Press 2014) 603
[1066] *Rogers v Secretary of State for the Home Department* (1973) AC 388; *D v NSPCC* (1978) AC 171
[1067] Also see *Burmah Oil Co Ltd v Bank of England* (1980) AC 1090; J. Alder, *Constitutional and Administrative Law* (10th ed, London, Palgrave 2015) 562
[1068] C. Rogers, R. Lewis, T. John, T. Read, *Police Work: Principles and Practice* (Abingdon, Routledge 2011) 132
[1069] B. Emmerson, A. Ashworth, A. Macdonald, *Human Rights and Criminal Justice* (3rd ed, London, Sweet & Maxwell 2012) 328
[1070] Ibid
[1071] Ibid

jurisdiction can be used and analogies can be drawn in reasoning.[1072] When intercept material has been legally obtained by virtue of sections 3 and 4 of RIPA, then it can be used.[1073] However, s.18 contains various measures, so that the court and prosecutor can discharge their duties in respect of Article 6 of the ECHR. S.18(7)(a) of RIPA states that the principle which proscribes disclosure does not apply when a prosecutor *"determine[s] what is required of him by his duty to secure the fairness of the prosecution."*[1074] Furthermore, sections 18(7)(b), 18(8) and 18(9) of RIPA empower the judge to order the prosecution to provide the material to him alone during a public interest immunity hearing, though only when there are *"exceptional circumstances"* and *"disclosure is essential in the interests of justice."*[1075]

S.18(10) enables the court after perusing the material to require the prosecutor to admit a fact, which is crucial to preserve justice, though the judge cannot require disclosure of the material or information about the way in which the material was obtained.[1076] As a result, only a *"constrained admission"* can be obtained and Emmerson et al doubt whether this ensures a fair hearing and argue that this does not comply with the decision in *Rowe and Davis v UK*[1077], in which it was established that equality of arms is required.[1078]

[1072] *R v Austin* (2009) EWCA Crim 1572; *R v Aujili* (1998) Cr App R 16; *R v X, Y and Z*, The Times, 23 May 2000; 329
[1073] S.18(4) of RIPA; B. Emmerson, A. Ashworth, A. Macdonald, *Human Rights and Criminal Justice* (3rd ed, London, Sweet & Maxwell 2012) 329
[1074] Emmerson et al (ibid)
[1075] Ibid
[1076] Ibid
[1077] (2000) 30 EHRR 1
[1078] B. Emmerson, A. Ashworth, A. Macdonald, *Human Rights and Criminal Justice* (3rd ed, London, Sweet & Maxwell 2012) 329

3.6 Summary

This chapter has shown that the UK has updated its cybercrime law regularly and new offences have been added, with a view to protecting critical infrastructure, which is vital in an age of cyber terrorism and warfare. Penalties have increased, so that cyber criminals can be convicted for life in very serious cases. This recognises that digital crimes can have as catastrophic consequences as physical crimes. It also acts as a deterrent. The law has also been aligned with EU law and the Cybercrime Convention, thereby resulting in a harmonisation. This is important to facilitate co-operation between enforcement agencies which often have to work together in order to bring cyber criminals to justice, who could otherwise easily exploit the borderless nature of the digital realm. The scope of jurisdiction has been widened, which is crucial to hold those to account who may reside outside of the UK, but perpetrate crimes within it, and extends to incorporate UK nationals who commit cybercrime in other countries whilst abroad.

Enforcement agencies have been given broad policing powers which helps them to prevent, detect and prosecute individuals for the commission of the various computer misuse offences. These powers have been put on a statutory footing and a governance framework has been adopted, so that these powers are not used in an arbitrary manner. Warrants have to be issued or judicial approval has to be sought for more intrusive

covert policing techniques. For instance, s.8(4) of RIPA requires that a warrant has to be granted for bulk data interception.

Interception, surveillance, communications data acquisition and decryption have thereby become key tools in the arsenal of enforcement agencies.

Certainly, the task of policing the digital space has become more challenging for the police and other enforcement agents, as they have to continuously keep up to date with innovation and new threats. These measures are therefore undoubtedly extremely valuable measures in the fight against cybercrime. They ensure that the many digital traces which cyber criminals may leave behind can be captured. This helps to secure the digital crime scene and forms part of a pro-active policing approach.

Without these powers, it would be extremely difficult to protect the public against the new threats from around the world. However, it is important that these powers are exercised in a lawful manner and comply with democratic values. This raises important questions about the justifiable degree of interference with fundamental rights and values, most notably the right to privacy, as highlighted by the Grand Chamber decision of the CJEU in *Digital Rights Ireland and Seitlinger and others*. Moreover, the public interest immunity protects the police from revealing their policing practices and thereby prevents their work from being undermined. However, this has an impact on the right to a fair hearing, and it is important that a careful balance is struck and that judges are given enough discretion to determine whether or not an application to have material excluded is warranted.

Chapter Four: The UAE's Legislative Framework to Combat E-Crime

4. Introduction

Cybercrime often takes place across borders and for this reason it is imperative that countries have the necessary tools to protect themselves.[1079] As the UAE has become a vibrant economic hub, has a very high take up of internet usage and ranked 6th in terms of e-participation and 7th in terms of online services in 2010[1080], it has also become a target of cybercrime attacks.[1081] A 2013 report by Symantec identified that around 17% of the entire population in the UAE had become affected by cybercrime.[1082] A 2014 report by PwC informed that cybercrime is the second highest economic crime with 41%, which is 4% higher than the global average.[1083] This highlights that cybercrime has remained a prevalent crime in the UAE.

Cyber attacks, for instance, in the form of denial of service, malware and phising, have increased and the IT security of government agencies have become targets, as well as

[1079] J. A. Lewis, G. Neuneck, United Nations Institute for Disarmament Research Report, The cyber index, International Security Trends and Realities, Center for Strategic and International Studies, 1-153, ix <http://www.unidir.org/files/publications/pdfs/cyber-index-2013-en-463.pdf> accessed 17th April 2016 2013

[1080] A. M. Al-Khouri, 'e-Government Strategies, The Case of the United Arab Emirates' (2012) 17 *European Journal of e-Practice*, 126-150, 134

[1081] S. S. Basamh, H. A. Qudaih, J. Bin Ibrahim, An overview on Cyber Security Awareness in Muslim Countries (2014) *International Journal of Information and Communication Technology*, 21-24, 21

[1082] Symantec, Internet Security Threat Report, 2013, 18

[1083] PwC, Economic Crime in the UAE, 2014, 1-6, 2

industrial data.[1084] In 2010 several customers of UAE Bank lost their savings due to internet fraud.[1085] Hence, financial services have been a particular target of cyber criminals.[1086] Cyber security is thus a national priority, including in light of the fact that the UAE is adopting a smart grid and is building its first nuclear plant in Barakah, which is scheduled to be ready by 2020.[1087] A digitised infrastructure creates security threats since systems are run on networks and with the help of software.[1088] It is for these reasons that it is essential that the legislative e-crime regime equips enforcement agencies with sufficient powers to keep the digital realm safe. This also necessitates a proactive policing approach, so that cyber security risks can be minimised before attacks take place.

The UAE government has already increased its budget in order to build and develop its cyber security capacity.[1089] In 2007, the UAE government launched the aeCERT security awareness campaign in order to safeguard online information and to block

[1084] A. Al Neaimi, 'A Critical Analysis of the Effectiveness of Cyber Security Defenses in UAE Government Agencies' (2014) *Proceedings of the International Conference on Information Security and Cyber Forensics*, Kuala Terengganu, Malaysia, 36-43, 36
[1085] F. Aloul, Information security awareness in UAE: A Survey paper (2010) Internet Technology and Secured Transactions, 1-6, 1
[1086] S. Paterson, B. Hopps, N. Lovell, United Arab Emirates, Cybersecurity, Herbert Smith Freehills LLP, 17 March 2016, 1-6, 2
[1087] A. McAuley, UAE nuclear project enters critical phase, the National, 7 July 2015 <http://www.thenational.ae/business/energy/uae-nuclear-project-enters-critical-phase> accessed 20th April 2016; A. Al Neaimi, 'A Critical Analysis of the Effectiveness of Cyber Security Defenses in UAE Government Agencies' (2014) *Proceedings of the International Conference on Information Security and Cyber Forensics*, Kuala Terengganu, Malaysia, 36-43, 37-38
[1088] K. Kwangjo, D. Kaist, Challenges of Cyber Security for Nuclear Power Plants, Khalifa University of Science, Technology and Research, Abu Dhabi, UAE, 18th Pacific Basin Nuclear Conference, BEXCO, Busan, Korea, 2012, 1-7, 1 <http://caislab.kaist.ac.kr/publication/paper_files/2012/PBNC2012-kkj.pdf> accessed 20th April 2016
[1089] Defense News, UAE to Double Security Budget, Focus on Cyber, 24 February 2014, Military Edge <http://militaryedge.org/articles/uae-double-security-budget-focus-cyber/> accessed 19th April 2016

immoral websites with a view of combating pornography and child abuse.[1090] Additionally, UAE police have created cybercrime units and computer forensic teams, who are experts in analysing electronic evidence.[1091]

An e-government strategic framework was adopted for the period 2012 to 2014 with a view of developing a knowledge-based economy though *"world class practices in all areas of e-government."*[1092] A secure identity management infrastructure has been adopted, which has made it possible to conduct secure e-government transactions and to link the electronic identity to the particular individual.[1093] Furthermore, government agencies have to also adhere to Cabinet Resolution No. 21 of 2012 concerning Information Security Regulations in the Federal Authorities, as well as Executive Council Resolution No.13 of 2012 regarding the Information Security in the Government of Dubai.[1094]

Moreover, the Telecommunications Regulatory Authority is responsible for telecommunications services, as well as the regulatory regime, including the internet access management policy.[1095] A policy sets out which online categories cannot be displayed by internet service providers and thus requires that access to certain content is

[1090] A. Al Neaimi, 'A Critical Analysis of the Effectiveness of Cyber Security Defenses in UAE Government Agencies' (2014) *Proceedings of the International Conference on Information Security and Cyber Forensics*, Kuala Terengganu, Malaysia, 36-43, 37
[1091] A. Al Neyadi, A. Al Kaabi, L. al Kabi, M. Al Ghufli, M. Al Sahmsi, M. Khan, 'Internet Governance & Cybercrimes in UAE (2015) 4(11) *International Journal of Scientific & Technology Research*, 350-357, 352
[1092] A. M. Al-Khouri, 'e-Government Strategies, The Case of the United Arab Emirates' (2012) 17 *European Journal of e-Practive*,126-150, 135-136
[1093] Al-Khouri (ibid) 126
[1094] S. Paterson, B. Hopps, N. Lovell, United Arab Emirates, Cybersecurity, Herbert Smith Freehills LLP, 17 March 2016, 1-6, 2
[1095] Telecommunications Regulatory Authority <http://www.tra.org.aw> accessed 17th April 2016

blocked, such as websites to malicious codes, phising webpages, sites where spy-software is downloaded, sites where illegal drugs are sold, gambling sites, sites with pornography, etc. In 2013, the Telecommunications Regulatory Authority also defended various government webpages against cyber attacks with the assistance of the Computer Emergency Response Team aeCERT.[1096] The Dubai Financial Services Authority is also trying to ensure that its regulatory rules comply with ISO 27032, which sets out guidance in respect of cyber security.[1097] Those, who are operating businesses in the Dubai International Financial Centre (DIFC), have a duty of care under Law No.2 of 2015 concerning Commercial Companies and DIFC Law No.5 of 2005 imposes a similar duty. Moreover, the Dubai Financial Service Authority requires that regulated entities adopt operating systems and checks in order to mitigate risks, which includes cyber attacks, and when this is not done, a fine can be imposed by the regulator.[1098]

Since 2012, the National Electronic Security Authority (NESA) is responsible for enhancing the national cyber security and critical information infrastructure.[1099] It has various competencies, ranging from suggesting the state's policy in the e-security field, and executing the same after its adoption; setting the state's e-security standards and supervising their execution; preparing a national plan to face any risks, threats or attacks on the e-security in coordination with the concerned parties; verifying the efficiency of the systems; protecting the communications network and information

[1096] UAE Computer Emergency Response Team <https://www.tra.gov.ae/aecert/en/media/news-archive/2015/3/31/the-tras-uae-computer-emergency-response-team-aecert-organizes-an-aviation-security-workshop.aspx> accessed 20th April 2016
[1097] S. Paterson, B. Hopps, N. Lovell, United Arab Emirates, Cybersecurity, Herbert Smith Freehills LLP, 17 March 2016, 1-6, 2
[1098] Paterson et al (ibid)
[1099] Law No. 3 of 2012 on Establishing the National Electronic Security Authority

systems of governmental and private bodies operating in the state; supervising the commitment of the concerned parties and the implementation of the e-security requirements issued by the Authority, and following up their implementation; fighting the crimes pertaining to computing, information network and information technology, of whatsoever type; coordinating with the regional and international concerned parties regarding the authority's scope of work; providing technical and advisory support; receiving complaints and suggestions; preparing and funding the necessary studies and research in coordination with the concerned parties; setting the required controls after coordinating with the concerned parties in the state, in order to authorise various activities, e.g. importing, exporting and using encryption and jamming hardware and software; testing the intrusion vulnerability of the communications network and information systems; suggesting legislations related to the e-security; spreading awareness; organising and participating in conferences and cooperating with regional and international organisations.[1100] The NESA has also issued various papers in order to improve security, such as the Critical Information Infrastructure Policy, the National Cyber Security Strategy and the Information Assurance Standards and some of these policies have as its base ISO 27001, which spells out the international standards for information security management systems.[1101]

Despite the various initiatives, El Guindy points out that the legislator and law enforcement agents face several challenges:[1102] Cybercrime offences form only one

[1100] Article 5 of Law No. 3 of 2012 on Establishing the National Electronic Security Authority
[1101] S. Paterson, B. Hopps, N. Lovell, United Arab Emirates, Cybersecurity, Herbert Smith Freehills LLP, 17 March 2016, 1-6, 2
[1102] M. N. El Guindy, Cybercrime challenges in the Middle East, 2012, Cyber Security, 1-6, 2

aspect of an effectiveanti-cybercrime strategy. It is therefore important that a more holistic approach is adopted in order to combat cybercrime effectively, particularly in light of the fact that even the existing cyber laws are relatively weak and unreliable, especially at the prosecution stage which raises much more complex procedural issues in comparison to traditional crimes.[1103] Challenges also exist because of insufficient technical capabilities, especially in relation to the procedural aspects of cybercrime investigations.[1104] It is essential that digital evidence is preserved and its integrity is ensured and this necessitates more sophisticated search and seizure criminal law procedures.[1105] Furthermore, as cyber-criminals may be located abroad, new technical capabilities have to be built, especially in the field of surveillance in order to track and identify criminals and this raises complicated questions in respect of the right to privacy and generally in terms of accountability.[1106] Another challenge is to create good organisational structures in order to facilitate co-operation, though in the UAE law enforcement officers already work together with the Computer Emergency Response Teams.[1107] However, it may also prove important if legislation would address the topic of cooperation with other stakeholders, including with the private sector, as well as regional and international cooperation.[1108] At the 5th International Cybercrimes Conference 2014 in Abu Dhabi, it was also recommended that law enforcement agencies, information technology regulatory authorities and judicial authorities should cooperate more and that the state should enter into partnership agreements with

[1103] Ibid (El Guindy)
[1104] Ibid (El Guindy)
[1105] A. T. S. Ho, *Handbook of Digital Forensics of Multimedia Data and Devices* (Chichester, John Wiley & Sons Ltd 2015) 95
[1106] M. N. El Guindy, Cybercrime challenges in the Middle East, 2012, Cyber Security, 1-6, 4
[1107] Ibid (El Guindy)
[1108] Ibid (El Guindy)

academic entities and the private sector.[1109] Furthermore, Al-Bawaba observes that *"cybercrime laws in the UAE are dangerously vague."*[1110] It has to be therefore analysed whether the existing e-crime provisions are sufficient in order to safeguard the national security interests of the UAE.

[1109] ME-Newswire, Cybercrimes Conference recommends establishing specialized prosecutions in federal and local courts, Abu Dhabi, UAE, 5 April 2014 <http://www.me-newswire.net/news/cyber-crimes-conference-recommends-establishing-specialized-prosecutions-in-federal-and-local-courts/en> accessed 26th April 2016

[1110] Al Bawaba, Cybercrime laws in the UAE are dangerously vague, 2012 <http://www.thefreelibrary.com/Cyber+crime+laws+in+the+UAE+are+dangerously+vague.-a0308238246> accessed 20th April 2016

4.1 The UAE's Legislative E-Crime Framework

The first law which the UAE adopted in order to specifically combat cybercrime was Federal Law No.2 of 2006 on combating cybercrime. This law contained 29 Articles which defined certain phrases and terms and set out various offences, including their punishment, particularly the issues of identity theft, internet fraud, hacking and causing harm to the public. For instance, Article 2 of Federal Law No.2 of 2006 provided that an *"international act whereby a person unlawfully gains access to a website or information system by logging on to the website or system or breaking through a security measure carried imprisonment or a fine or either."* Those who facilitated or committed these offences could be imprisoned for a longer term or be required to pay a higher fine.[1111] Internet fraud was further rendered illegal by virtue of Article 10, which stated that anyone who *"through the internet or the computer appropriates to himself or to another moveable property or procures a deed or signature upon a deed, using deception, a false name or impersonation with intent to defraud the victim, shall be liable to imprisonment for a term of at least one year and a fine of at least AED 30,000."* Furthermore, Article 11 made clear that anyone *"who uses the internet or computer to unlawfully access the number or details of a credit card or other electronic card shall be liable to imprisonment and a fine..."* Moreover, *"a person who unlawfully logs on to an internet website in order to change, delete, destroy or modify its design or take over its address shall be liable to imprisonment and a fine or either of the two."*[1112]

[1111] Article 3 of Federal Law No.2 of on combating cybercrimes
[1112] Article 14 of Federal Law No.2 of 2006 on combating cybercrime

Not all cybercrimes are motivated by financial gain, for instance, worms and viruses i.e. malicious software simply cause financial loss.[1113] Another typical cybercrime is hacking i.e. gaining illegal access to a system without having an authority and this can be done for various purposes, including to commit identity theft, vandalism, to spread political ideas, etc. The law therefore also imposed very strict penalties for these kinds of offences, including arguably spam and viruses.[1114] Article 5 provided that *"a person who in any way hinders or delays access to a service, system, server or database through the internet or computer shall be liable to imprisonment and a fine."* Another Article which addressed the threat emanating from viruses, worms and hacking was Article 6. This Article made clear that *"a person who uses the internet or computer in order to disable, destroy, wipeout, delete, damage, or modify programs, data or information on the internet or computer shall be liable to temporary detention and a fine of not less than AED 50,000 or either of the two."* However, this provision was insufficient to address information security issues in respect of cloud computing i.e. failed to explain whether a cloud provider, who does not protect its user, is responsible for the injuries caused by a hacker; and users of clouds, who suffered losses as a result of it, had to rely on the contractual provisions and the civil law.[1115]

Federal Law No.2 of 2006 on combating cybercrime also criminalised acts which caused harm to the public or persons, such as online extortion, stalking, blackmail and defamation. For instance, Article 9 outlawed blackmail and threatening another through

[1113] R. Sinn, *Software Security Technologies, A Programmatic Approach* (Stamford, Cengage Learning 2008) 41
[1114] C. Khan, Caught in the net, *The Brief*, November 2009, 23-24, 24
[1115] S. Paterson, B. Hopps, N. Lovell, United Arab Emirates, Cybersecurity, Herbert Smith Freehills LLP, 17 March 2016, 1-6, 3

the use of a computer or the internet and rendered it a crime punishable by *"imprisonment for up to two years and a fine not exceeding AED 50,000 or either of the two."* Another provision which combated that the internet was used to defame others was Article 16, which proscribed that the internet or a computer was used to breach family values and principles, or to publish pictures or news which invade the privacy of a person or their family life, even if they are accurate, and rendered this a crime punishable with at least one-year imprisonment and *"a fine of at least AED 50,000 or either of the two."* Yet the law did not clarify what constitutes family values and principles, as well as what information should be considered private. This is despite the fact that this is an important issue, as it is difficult to police the digital realm without surveillance.[1116] Hence, there existed a problem since any type of government surveillance arguably contravened Article 16, particularly since surveillance results in the internet or a computer being used to invade the privacy of a person. However, the provision did not contain a caveat which clarified that surveillance by enforcement agencies did not breach this provision. Also, the fact that online defamation was always considered a criminal offence was a draconian approach.

The Law also outlawed other crimes which harm public morality, such as internet gambling, pornography, paedophilia, drug and human trafficking, as well as cyber terrorism.[1117] The provisions were therefore very far-reaching in scope. Furthermore, individuals who distributed *"information that is contrary to public morals or operates a*

[1116] S. Jenkins, Blanket digital surveillance is a start. But how about a camera in every bathroom? The Guardian, 17 July 2014 <http://www.theguardian.com/commentisfree/2014/jul/17/blanket-digital-surveillance-is-a-start-but-how-about-a-camera-in-every-bathroom> accessed 25th April 2016
[1117] C. Khan, Caught in the net, *The Brief*, November 2009, 23-24, 24

venue for such purposes" could be imprisoned for at least six months and be made to pay AED 30,000 (approximately £5,659).[1118] Yet it would have been better if the concept of public morality had been further clarified in order to prevent a too broad construction. Without this, freedom of expression was stymied. Those who lured, incited or assisted females or males to engage in fornication or prostitution via a computer or the internet could also be criminally pursued and when this involved a minor, this attracted a minimum prison sentence of five years.[1119] Those, who engaged in human trafficking or the sale of mind altering substances or narcotics could also be temporarily detained.[1120] Those, who published information or created a website for terrorist groups, could be imprisoned for a maximum of five years.[1121]

This first cybercrime law was certainly an important stepping stone to combat cybercrime, but in light of the increase in cybercrime, it was considered a top priority to further strengthen the e-crime framework.[1122] In this context, the Head of the UAE Finance Public Prosecution, Counsellor Hassan Mohammed Al Hammadi observed that *"[t]he lawmaker issued the Federal Law No.2 of 2006 on combating the cybercrimes, but practical reality proved the statute had failed to keep in line with the rapid*

[1118] Article 12 of Federal Law No.2 of 2006 on combating cybercrime
[1119] Article 14 of Federal Law No.2 of 2006 on combating cybercrime
[1120] Articles 17-18 of Federal Law No.2 of 2006 on combating cybercrime
[1121] Article 21 of Federal Law No.2 of 2006 on combating cybercrime
[1122] J. Beretta, UAE Issues New Cybercrimes Law and Establishes a National E-Security Authority, Dentons, 7 January 2013 <http://www.dentons.com/en/insights/articles/2013/january/7/uae-issues-new-cyber-crimes-law-and-establishes-a-national-esecurity-authority> accessed 23rd April 2016

developments and the ensuing risks due to the amazing progress in modern technologies."[1123]

In 2012, the UAE therefore adopted Federal Law No. 5 of 2012 concerning Combating Information Technology Crimes, which replaced Federal Law No.2 of 2006 on combating cybercrime. This law has a total of 51 provisions, which proscribe a wider range of cybercrime offences. Federal Law No. 5 of 2012 also broadens the definition in respect of privacy violations by proscribing transmitting and disclosing audio and visual communications, taking photographs of individuals and saving, copying or publishing them, publishing statements, comments, news and information, including genuine and true information, and eavesdropping.[1124] Federal Law No. 5 of 2012 also increases privacy protection for credit card and bank account numbers, electronic payment methods and other online data.[1125] Yet the concept of *"privacy"* has not been defined and is therefore very wide.[1126] The interplay with Article 31 of the constitution, which also contains a right to privacy and confirms that communications are confidential whether sent by post or through other means, is not yet clear. Federal Law No.3 of 1987 (the penal code) also contains provisions which safeguard privacy, and which may be pleaded alongside the cybercrime provisions. For instance, Article 372 proscribes the publication of anything that causes contempt or hatred about a person. Article 373

[1123] M. Al Zarooni, Most e-crimes from across UAE border, Khaleej Times, 27 September 2013 <http://www.khaleejtimes.com/nation/crime/most-e-crimes-from-across-uae-border> accessed 26th April 2016

[1124] S. Saleem, New Law Combating Information Technology crimes, 2013, Tamimi <http://www.tamimi.com/en/magazine/law-update/section-5/january-2/new-law-combating-information-technology-crimes.html> accessed 21st April 2016

[1125] A. Al Neyadi, A. Al Kaabi, L. al Kabi, M. Al Ghufli, M. Al Sahmsi, M. Khan, 'Internet Governance & Cybercrimes in UAE (2015) 4(11) *International Journal of Scientific & Technology Research*, 350-357, 352

[1126] P. Beheshti, Keeping IT safe (2016) *Emirates Law Business & Practice*, 5-7, 7

renders it a criminal offence to falsely accuse a person in a way which discredits or dishonours him. It is also a crime to publish pictures, comments or news which disclose information about the family or private lives of individuals, even when the information is accurate and it is in the public interest to do so. Yet Federal Law No.5 of 2012 is even wider since under the penal code it is necessary to show that the person possessed an intention to cause harm or to disclose private information.[1127] However, it is concerning that, for example, taking photographs of individuals and saving, copying or publishing them or publishing genuine information, can constitute a criminal offence. It does not send out the message of being a moderate Islamic country. It is therefore important that scholars develop the necessary caveats and exceptions. Guidance should be published to distinguish criminal conduct from, e.g. the harmless practice of posting pictures of friends on social media. Otherwise, the risk is that individuals are being convicted without having engaged in morally culpable conduct.

Whilst the right to privacy has been protected by virtue of the criminal law, there exist no other data protection legislation, apart from data protection legislation which applies in the DIFC[1128] and to a certain extent Federal Law No.6 of 2010 concerning credit information. This latter law imposes obligations on financial institutions and commercial banks to keep data confidential and to seek the consent of the data subject prior to any disclosure. A failure to adhere to this can result in criminal sanctions being

[1127] P. Beheshti, V. Hambly, 'To Post...or Not to Post?' (2016) *Emirates Law Business & Practice*, 23-24, 23

[1128] S. Paterson, B. Hopps, N. Lovell, United Arab Emirates, Cybersecurity, Herbert Smith Freehills LLP, 17 March 2016, 1-6, 2

imposed under Federal Law No.3 of 1987 (the penal code).[1129] Nonetheless, the data protection legislation of the DIFC does not apply to the rest of the UAE and Federal Law No. 5 of 2012 does not spell out any rights and remedies for data subjects.[1130] Accordingly, the legislator has not utilised the concept of data protection fully to render the digital realm safer, e.g. by requiring businesses to collect only as much data as is necessary, as this safeguards citizens against cyber-security incidents.[1131] In this context, it must also be stressed that the legislator should consider privacy intrusions civil matters, except in serious cases. Nonetheless, Federal Law No. 5 of 2012 concerning Combating Information Technology Crimes certainly enhances protection against crime committed on the internet and on other digital devices and also increases the legal arsenal of tools to safeguard sensitive and confidential information more effectively.[1132] However, just like its predecessor, the 2012 law does not define cybercrime. This appears to be a sensible approach, as a specific definition may become outdated in light of rapid technological and criminal innovation. Indeed, Federal Law No. 5 of 2012 refines the cybercrime offences. For instance, Article 2 of Federal Law No.2 of 2006 required that it was shown that the accused had an intention to wilfully access an information system or website or to overstep authorised access, but Federal Law No. 5 of 2012 no longer requires this.[1133] Hence, it has become much easier to prosecute cyber criminals, as no *mens rea* has to be proven beyond reasonable doubt. The reach of the law has also been extended so that electronic sites, e.g. personal webpages, blogs and

[1129] Ibid (Paterson et al) 2
[1130] P. Beheshti, Keeping IT safe (2016) *Emirates Law Business & Practice*, 5-7, 7
[1131] European Commission, The EU's Data Protection rules and Cyber Security Strategy: two sides of the same coin, Luxembourg, 19 May 2013 <http://europa.eu/rapid/press-release_SPEECH-13-436_en.htm> accessed 28th April 2016
[1132] S. Paterson, B. Hopps, N. Lovell, United Arab Emirates, Cybersecurity, Herbert Smith Freehills LLP, 17 March 2016, 1-6, 3
[1133] P. Beheshti, Keeping IT safe (2016) *Emirates Law Business & Practice*, 5-7, 5

social networking sites, are expressly covered.[1134] Federal Law No. 5 of 2012 also imposes stricter penalties in comparison to Federal Law No.2 of 2006, which only imposed prison sentences for up to seven years and the fines also only ranged from AED 20,000 (approximately £3,700) to AED 50,000 (approximately £9,400).[1135]

Federal Law No. 5 of 2012 deals with the following broad categories: IT security, political stability and state security, proper conduct and morality, commercial and financial issues and miscellaneous matters.[1136] The Articles which deal with IT security now outlaw a broader range of issues, such as hacking, changing webpages, distributing viruses and stealing data. Article 2 deals with the issue of accessing IT systems without having any authority and the sanctions are increased in case this concerns personal data or when this is done by an employee. Article 4 addresses the issue of accessing IT system without authority in order to obtain commercial or government information. Article 5 renders it illegal to access a webpage without having permission in order to delete, change or damage the content. Article 8 addresses the problem of disabling access, so that others cannot access the IT system. Article 9 criminalises the fraudulent use of a computer network protocol by using a false address or third-party address in order to commit a crime or prevent its discovery. Yet the issue with this provision is that it is very wide and can cover instances where an IP address is masked for hacking purposes, but could also cover use of off-shore virtual private network (VPN) in order to

[1134] Beheshti (ibid)
[1135] F. Cassim, 'Formulating specialised legislation to address the growing spectre of cybercrime: a comparative study' (2009) 12(4) *Scielo* [online] <http://www.scielo.org.za/scielo.php?script=sci_arttext&pid=S1727-37812009000400004> accessed 27th April 2016
[1136] N. O'Connell, Developments in the UAE Cybercrimes Law, May 2013, Tamimi <http://www.tamimi.com/en/magazine/law-update/section-5/may-5/developments-in-the-uae-cyber-crimes-law.html> accessed 23rd April 2016

access blocked content.[1137] However, clearly use of a VPN should not attract the same punishment as hacking.

Introducing virus programmes and spam emails[1138]; obtaining passwords without authority[1139]; intercepting communications through IT systems without authority[1140]; and disclosing confidential information without authority through IT systems[1141] have also been criminalised and sanctions have been spelled out.

Political stability and state security are safeguarded through the criminalisation of the following acts: Gaining access without authority to commercial or government information[1142]; posting online or operating a site which causes racism, hatred, sectarianism, sedition, undermining social peace or national unity or harming public morals or the public order[1143]; posting information or operating a site for an illegal organisation or a terrorist group;[1144] posting information online or operating a site which endangers and harms the public order or reveals state security[1145]; publishing rumours, news or information online in order to harm the state[1146]; posting information online or operating a site to undermine the constitution or overthrow the government[1147];

[1137] N. O'Connell, 'Cyber Security & Data Protection, Roles & Responsibilities' (2016) *Emirates Law Business & Practice*, 16-18, 17
[1138] Article 10 of Federal Law No. 5 of 2012 Concerning Combating Information Technology Crimes
[1139] Article 14 of Federal Law No. 5 of 2012 Concerning Combating Information Technology Crimes
[1140] Article 15 of Federal Law No. 5 of 2012 Concerning Combating Information Technology Crimes
[1141] Article 22 of Federal Law No. 5 of 2012 Concerning Combating Information Technology Crimes
[1142] Article 4 of Federal Law No. 5 of 2012 Concerning Combating Information Technology Crimes
[1143] Article 24 of Federal Law No. 5 of 2012 Concerning Combating Information Technology Crimes
[1144] Article 26 of Federal Law No. 5 of 2012 Concerning Combating Information Technology Crimes
[1145] Article 28 of Federal Law No. 5 of 2012 Concerning Combating Information Technology Crimes
[1146] Article 29 of Federal Law No. 5 of 2012 Concerning Combating Information Technology Crimes
[1147] Article 30 of Federal Law No. 5 of 2012 Concerning Combating Information Technology Crimes

publishing information on the internet which promotes non-adherence with laws[1148]; and employing an IT system to furnish others with data which contravenes the dignity or interest of the state.[1149]

Proper conduct and morality on the internet are enforced through rendering it a crime to run or manage a website or publish, send or transmit pornographic material, gambling activities and whatever that which may afflict the public morals[1150]; to entice, aid, abet or engage in lewdness or prostitution by using a computer network or any information technology means[1151]; to slander[1152]; to violate the privacy of others, e.g. through photos, intercepting communications, publishing information[1153]; and to encourage sins, offend Islamic rituals and insult recognised religions.[1154] As observed above, criminalising privacy intrusion is a draconian approach.

A 2013 Federal Supreme Court case[1155] also illustrates that the provisions of Federal Law No.5 of 2012 may raise legal issues. This case concerned how Article 20 of Federal Law No.5 of 2012 should be interpreted. Article 20 provides that

> *"Without prejudice to the provisions of the crime of defamation prescribed for under Islamic Sharia, any person who insults another person or assigns to another person an incident which makes such person a subject of*

[1148] Article 31 of Federal Law No. 5 of 2012 Concerning Combating Information Technology Crimes
[1149] Article 38 of Federal Law No. 5 of 2012 Concerning Combating Information Technology Crimes
[1150] Article 17 of Federal Law No. 5 of 2012 Concerning Combating Information Technology Crimes
[1151] Article 19 of Federal Law No. 5 of 2012 Concerning Combating Information Technology Crimes
[1152] Article 20 of Federal Law No. 5 of 2012 Concerning Combating Information Technology Crimes
[1153] Article 21 of Federal Law No. 5 of 2012 Concerning Combating Information Technology Crimes
[1154] Article 35 of Federal Law No. 5 of 2012 Concerning Combating Information Technology Crimes
[1155] Supreme No. 345/2013

contempt by others through the use of website or means of information technology, shall be punished by imprisonment and a fine of no less than two hundred fifty thousand dirham and not exceeding five hundred thousand dirham or by either of these two penalties, and if the insult or defamation is against a public servant or a person assigned to public service on a certain occasion or during the performance of his job, the same shall be considered as an aggravating circumstances for the crime."

In this case, the second and third accused made statements about a Headmistress, which were defamatory i.e. negatively commented on her job performance on a website. The first accused assisted the second and third accused in committing the crime. The public prosecutor charged the second and third accused by virtue of Articles 45 and 47 of the Penal Code and Articles 1, 20 and 41 of Law No.5 of 2012. The Court of First Instance decided that each accused should be fined and their blackberry devices should be confiscated. The three accused appealed and the Fujairah Court of Appeal accepted the appeals and lowered the fines to AED 3,000 each, but otherwise upheld the judgment. The second and third accused nonetheless appealed the decision. The office of public prosecution lodged a memo in which it requested that this renewed challenge is dismissed. The two appellants challenged the decision on the basis that the law was wrongly applied since the words employed did not amount to contempt by others and that they only raised questions and also did not mention the name of the person. They particularly averred that it was wrong to evoke Article 20 of Law No. 5 of 2012 concerning Combating Information Technology Crimes and that this renders the entire

decision defective. The Supreme Court stated that the principle is that it is up to the judge to be satisfied from the facts of the case and that so long as the judge did not wrongly apply the law to the facts, no challenge can be brought. Moreover, by law the court has to identify the person who has been defamed and insulted and analyse whether the words of insult have been directed at him/her and the circumstances have to be considered in order to ascertain whether there were any reservations or whether the name of the victim was not expressly mentioned. If it was clear to the court that the accused intended to insult the person, then this cannot be further challenged. In the instance case, the words, which were published through a Blackberry device owned by the accused, clearly made the Headmistress a subject of contempt through the published words and expressions. The law was therefore correctly applied, as the words were insulting, defamatory and degrading and undermined the person's dignity in the eyes of other people. The Court therefore ruled that the appeal of the appellants on the basis that Article 20 did not apply was baseless. This case highlights that it may be useful that the various sections of Federal Law No.5 of 2012 are clarified, for instance, guidance could be issued in order to avoid that the law is considered vague and ambiguous, as well as to provide further directions to the judiciary, as well as prosecutors. Also, it should be debated whether defamation cases should be considered civil, as opposed to criminal cases. This may also prove important in order to avoid criticism, e.g. by Amnesty International, that the new cybercrime law is being used to unduly curtail freedom of expression.[1156]

[1156] Amnesty International, United Arab Emirates 201/2016 <https://www.amnesty.org/en/countries/middle-east-and-north-africa/united-arab-emirates/report-united-arab-emirates/> accessed 29th April 2016

Cybercrimes relating to the commercial and financial sector are generally addressed through provisions dealing with financial matters and ecommerce, such as committing forgery of electronic documents[1157]; using fraudulent means through the computer network to obtain benefits, personal property or signatures[1158]; gaining access without authority to electronic or credit card number, bank accounts or data or other electronic payment methods through information technology, electronic information systems or computer networks[1159]; forging, reproducing, counterfeiting debit or credit cards or other electronic payment methods.[1160]Additionally, the law addresses various miscellaneous matters, such as using blackmail to coerce someone into engaging in illegal behaviour.[1161]

Article 47 also ensures that the law has extra-territorial application since it provides that:

> "*the provisions of this Decree Law shall apply to any person who has committed any of the crimes mentioned therein outside the country, if its object is an electronic information system, computer network, website or information technology means relates to the federal government or any of the local governments of the Emirates of the State or any authority or public institution owned by any of them."*

[1157] Article 6 of Federal Law No. 5 of 2012 Concerning Combating Information Technology Crimes
[1158] Article 11 of Federal Law No. 5 of 2012 Concerning Combating Information Technology Crimes
[1159] Article 12 of Federal Law No. 5 of 2012 Concerning Combating Information Technology Crimes
[1160] Article 13 of Federal Law No. 5 of 2012 Concerning Combating Information Technology Crimes
[1161] Article 16 of Federal Law No. 5 of 2012 Concerning Combating Information Technology Crimes

It becomes increasingly clear from the wording of this section, extra-territoriality only applies when a cybercrime is directed against the state. Although it is probably better to adopt a wider approach, e.g. by assuming that *"all crime is local."*[1162] Hence, the adoption of a concept of *"territoriality"* could circumvent the difficult questions which arise from extra-territoriality.[1163] This arguably also accords with the Penal Code, which contains provisions which provide for extra-territoriality when one of the elements which make up the crime has taken place on the state territory or if it has had a result on the state territory.[1164] It may therefore be argued that all of the cybercrime offences have extra-territorial effect.[1165] However, the trend is rather to provide for extensive extra-territorial powers and it may therefore be best not to restrict the enforcement of Federal Law No. 5 of 2012 to only cybercrimes which have been committed against emanations of the state.[1166] It may therefore be useful if specific guidance was developed for public prosecutor in order to clarify this issue, as it falls on public prosecutors to determine whether proceedings should be brought when crimes have been committed by persons abroad.[1167] For instance, relevant threshold amounts could be set, as well as particular crimes could be classified as serious, e.g. attacks against critical national infrastructure, and these could then trigger automatic legal action against cyber criminals, who are located abroad. At the same time, the UAE should try and enter into extradition treaties with other countries, so that the extraterritorial reach of Federal Law No. 5 of 2012

[1162] R. Broadhurst, P. Grabosky, *Cyber-Crime: The Challenge in Asia* (Hong Kong, Hong Kong University Press 2005) 154
[1163] Broadhurst and Grabosky (ibid)
[1164] N. O'Connell, 'Cyber Security & Data Protection, Roles & Responsibilities' (2016) *Emirates Law Business & Practice*, 16-18, 17
[1165] O'Connell (ibid) 17
[1166] R. Broadhurst, P. Grabosky, *Cyber-Crime: The Challenge in Asia* (Hong Kong, Hong Kong University Press 2005) 154
[1167] O'Connell (ibid) 17

becomes a more effective deterrent against cyber criminals located abroad.[1168] Without such steps, the problem is that most cybercrime offences cannot be investigated if they have not been committed against the state and took place abroad, which is mostly the case.

In terms of the penalties, cyber criminals can be imprisoned, fines can be imposed and foreigners can also be deported.[1169] Some of the offences attract life imprisonment, e.g. undermining the regime, and hefty fines, e.g. sending viruses can be punished with up to AED 3 million (approximately £565,000).[1170] Devices, programs or other means used to perpetrate the crime can also be confiscated, as well as money and information and statements can be deleted and the court can also order that sites or domains are closed permanently or temporarily.[1171] Those, who have been convicted under the law, can also be deprived of the right to use any computer network or electronic information system or any other information technology means, and a person can also be sent to a rehabilitation centre for a period which the court considers appropriate.[1172]

Federal Law No.5 of 2012 certainly protects the UAE against a wide range of cybercrimes. It clarifies the various crimes and ensures that there exists legal certainty, also because the penalties have been clearly spelled out. Yet some of the provisions are

[1168] J. Keane, This ain't CSI: How the FBI Hunts Down Cyber Criminals Around the Globe, Digital Trends, 2 August 2015 <http://www.digitaltrends.com/computing/how-the-fbi-hunts-down-cyber-criminals-around-the-globe/> accessed 29th April 2016
[1169] Article 42 of Federal Law No. 5 of 2012 Concerning Combating Information Technology Crimes
[1170] P. Beheshti, Keeping IT safe (2016) *Emirates Law Business & Practice*, 5-7, 6
[1171] Article 41 of Federal Law No. 5 of 2012 Concerning Combating Information Technology Crimes
[1172] Article 43 of Federal Law No. 5 of 2012 Concerning Combating Information Technology Crimes

framed in very broad terms, for instance, it is illegal to record conversations.[1173] In the future, it is therefore important to ensure that the law is not interpreted in a way which results in individuals, who have no intention to commit any crime, being prosecuted under this law.[1174] Statutory exceptions must therefore be created, or guidance must be published. Without such steps being taken, the problem is that the law has an overreach, which may result in innocent behaviour being unfairly punished. Also, whilst on the one hand many of the provisions are unduly broad, this cannot be said of Article 47 which confers extra-territorial application. The deterrent character of the cybercrime offences has thereby been also diminished since cyber criminals who are located abroad are unlikely to be pursued. This sends out the wrong message, namely that individuals located in the UAE who may not even have committed crimes are prosecuted (e.g. for taking a picture of another and publishing it), whereas serious cyber criminals located abroad are not pursued.

Whilst Federal Law No.5 of 2012 ensures that the cybercrime regime is much more comprehensive, there are still certain gaps. Fundamentally, it does not grant a power to law enforcement agents to conduct surveillance prior to any offence having taken place. Instead Article 43 states that *"the court may order to put the condemned under surveillance"*, but this does not permit a proactive policing approach. Yet the Department of Anti-Electronic Crimes and Abu Dhabi's State Security Apparatus, as

[1173] P. Beheshti, Keeping IT safe (2016) *Emirates Law Business & Practice*, 5-7, 5
[1174] Beheshti (ibid)

well as the police conduct surveillance.[1175] For instance, it has been reported that the UAE entered into contracts with various security firms in 2008 in order to meet its security needs and to create a *"mass civil surveillance system"*, including to safeguard civil surveillance systems and oil installations. [1176] Etisalat, the national telecommunications company, has also worked with the government, so that blackberries have a surveillance malware installed.[1177] Also, in November 2015, a press release on the webpage of the security and defence company Saab announced that the UAE had entered into a USD 1.27 billion contract in order to expand its surveillance capabilities.[1178] Yet as pointed out by the United Nations' Special Rapporteur, mass electronic surveillance breaches privacy rights set out in various conventions and treaties.[1179] It is therefore important for the UAE to adopt cybercrime legislation which equips law enforcement agents with the power to conduct surveillance, but which also contains the necessary safeguards against abuse. This also necessitates that the law addresses the scope of the surveillance powers and its relationship with the constitutionally guaranteed right to privacy.

[1175] A. Al Neyadi, A. Al Kaabi, L. al Kabi, M. Al Ghufli, M. Al Sahmsi, M. Khan, 'Internet Governance & Cybercrimes in UAE (2015) 4(11) *International Journal of Scientific & Technology Research*, 350-357, 352

[1176] R. Donaghy, Falcon Eye: The Israeli-installed mass civil surveillance system of Abu Dhabi, Middle East Eye, 28 February 2015 <http://www.middleeasteye.net/news/uae-israel-surveillance-2104952769> accessed 29th April 2016

[1177] M. Sutton, UAE Signs Deal to Integrate National IDs into Mobile Phones, Electronic Frontier Foundation, 12 April 2012 <https://www.eff.org/deeplinks/2012/04/uae-signs-deal-integrate-national-ids-mobile-phones> accessed 29th April 2016

[1178] Saab, Saab receives order for new advanced airborne surveillance systems from UAE, 10 November 2015 <http://saabgroup.com/media/news-press/news/2015-11/saab-receives-order-for-new-advanced-airborne-surveillance-systems-from-uae/> accessed 28th April 2016

[1179] United Nations General Assembly, Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Sixty-ninth session, 23 September 2014; G. Greenwald, UN Reports Finds Mass Surveillance Violates International Treaties and Privacy Rights, The Intercept, 15 October 2014 <https://theintercept.com/2014/10/15/un-investigator-report-condemns-mass-surveillance/> accessed 27th April 2016

Furthermore, Federal Law No.5 of 2012 does not impose a requirement to share information about cyber attacks or to notify the regulator, though Federal Law No.3 of 1987 (the penal code) renders it a criminal offence not to notify crimes.[1180] The e-crime legislation also fails to address how intellectual property is protected against cyber attacks[1181], though intellectual property is generally protected and civil and criminal sanctions can be imposed.[1182] There is also no specific crime for launching cyber attacks against critical infrastructure, as in the UK, as discussed in the previous chapter. It would therefore be useful for the law to add additional offences.

Moreover, regional cooperation is essential to combat cybercrime. It is therefore important to increase efforts to utilise the mechanisms which have been created by virtue of the Arab Convention on Combating Information Technology Offences 2010 (the "Arab Convention"). The purpose of the Arab Convention is to enhance and strengthen cooperation between the Arab States in the area of combating information technology offences to ward off the threats of such crimes in order to protect the security and interests of the Arab States and the safety of their communities and individuals. It attempts to implement in the national legislation of the States which have adopted this (such as Jordan, UAE, Sudan, Iraq, Palestine, Qatar, Kuwait and Oman) provisions that criminalise a set of online offenses as well as incorporate procedural rules fascilitating the prosecution of cybercrimes and the collection of digital evidence.

[1180] S. Paterson, B. Hopps, N. Lovell, United Arab Emirates, Cybersecurity, Herbert Smith Freehills LLP, 17 March 2016, 1-6, 4
[1181] Paterson et al (ibid), 3
[1182] Federal Law No. 37 of 1992, as amended by Law No. 19 of 2000 and Law No.8 of 2002 concerning Trade Marks; Federal Law No. 7 of 2002 in respect of author copyright and parallel rights; and Federal Law No. 17 of 2002, as amended by Federal Law No. 31 of 2006 concerning the protection of industrial property law

The treaty also has a section for promoting and enhancing the cooperation between its members in dealing with transnational cybercrimes[1183]. Yet the provisions in the Arab Convention which detail the requisite procedures have not been transposed by UAE law. At a 2012 conference in Doha, it was also reported that only eight out of the twenty-two Arab countries had set up national Computer Security Incident Response Teams/Computer Emergency Response Teams and that at the regional level they were not cooperating with each other.[1184] However, the Cooperation Council for the Arab States of the Gulf, namely, the UAE, Qatar, Saudi Arabia, Oman and Bahrain, already cooperate with each other.[1185] The Organisation of Islamic Cooperation, which has eighteen member countries, has also created a Computer Emergency Response Team or Computer Security and Incident Response Team.[1186] Nonetheless, for regional cooperation to be effective, the national response team and enforcement agencies must also follow the stipulated procedures and which should be put on a statutory footing.

The e-crime framework of the UAE is quite robust when it comes to the available offences and the various government initiatives have ensured a relatively high degree of protection. However, the cybercrime offences depend on the enforcement agents being able to collect digital evidence on which a prosecution can be founded. It is therefore important that digital evidence and the underlying procedural rules relating to digital evidence are not overlooked. The next section therefore analyses the UAE's Criminal Procedure Law, which governs also electronic evidence.

[1183] Arab Convention on Combating Information Technology Offences 2010.
[1184] Connect Arab Summit, Building trust and security in the use of ICTs, Background paper, 15 February 2012, 1-8, 3
[1185] Connect Arab Summit (ibid) 3
[1186] Connect Arab Summit (ibid) 3

4.2 The Criminal Procedure Law and Procedural Rules Governing Electronic Evidence

The UAE is a very modern state and its citizens make constant use of electronic devices. When cybercrime is committed, it is vital that there are clear procedural rules in place for electronic evidence. The UAE Criminal Procedural Law Federal Law No. 35 of 1992 is the relevant law in this area. This law spells out the relevant procedures for all criminal cases. It must be analysed whether the existing law is adequate when it comes to the collection of electronic evidence or whether it is necessary to adopt additional provisions.

Under the Criminal Procedure Law, an investigation has three phases: During the first phase, evidence is collected, then an initial investigation takes place and finally, a hearing is conducted. Judges can determine whether evidence should be admitted. Evidence is crucial in order to link the criminal to the offence. The relevant cybercrime offences and remedies are spelled out by statutes, as discussed above. Judges enjoy much discretion when it comes to deciding what evidence is admissible. However, they are not allowed to decide cases based on subjectively held beliefs.

Judges have to apply the relevant laws and *"discretionary interpretation"* is thus not allowed when there is a particular law, but when an issue is not addressed, judges make

use of general principles of justice and Islam and the Sharia.[1187] Yet whilst judges do not have to provide reasons for a particular decision, this is normally done in practice and may even form the subject matter of an appeal. Judges may also consider other cases which have addressed a particular issue. However, there are no publicly available cases and there exists no formal system of judicial precedent.[1188] Nonetheless, lower courts normally follow the decisions of higher courts.[1189]

Also, a judge does not have to justify why evidence has been used. No facts have to be established, so long as the decision is based on evidence. This is further illustrated by a 2011 Federal Supreme Court case.[1190] In this case, two accused were charged for deliberately exploiting a service of Etisalat by illegally entering and logging onto the Etisalat network in order to make international calls in a manner which violates Articles 1, 7, 42(2), 72 and 76 of Federal Law No.3 of 2003, as amended by Federal Law No.5 of 2007 regarding the regulation of Etisalat and the communications sector. The First Instance Court acquitted the accused. The public prosecutor appealed the decision and the appeal was accepted, though the decision confirmed the previous decision. The public prosecutor brought another appeal on the basis that bad reasoning had been employed and that the law had been wrongly applied. Reliance was placed on the accused confessing that they had inserted/installed a program on a phone through which they could make international calls for the same rate as local calls. A witness had also

[1187] Gulf-Law.com, Background on the United Arab Emirates (UAE) Legal System, 2014 <http://gulf-law.com/uaecolaw_legalsystem.html> accessed 3rd April 2016
[1188] Oxford Business Group, *The Report: Abu Dhabi 2010* (Oxford, Oxford Business Group 2010) 223
[1189] Ibid
[1190] Supreme No. 185/2011

confirmed that he had seen many people entering the room of the suspects in order to make international calls.

The Federal Supreme Court ruled that the two previous courts had reviewed all the circumstances, had studied and scrutinised the evidence and had weighed it and compared it with the evidence of the prosecution and had come to the conclusion that the two accused should be acquitted. Hence, a court can acquit a person on the basis that it suspects that the charge is invalid or there is insufficient evidence. Also, a court can acquit a person when not all the elements of a crime have been proven, as this renders a charge invalid. In these circumstances, the appeal by the public prosecutor was misperceived and was therefore dismissed. Hence, the case illustrates the important role which evidence plays, as insufficient evidence will result in an accused not being charged. In light of the fact that cybercrime is technically more challenging to prove, it is important that procedural rules are established in order to avoid that cyber criminals escape their just punishment merely because of evidence having become inadmissible or being weak.

Moreover, judges follow the principle of judicial understanding and this also bestows them with freedom to accept evidence as proof. Article 209 of the Criminal Procedure Law empowers judges to decide which evidence is important. In this context, an unpublished Federal Criminal Case[1191] clarifies in respect of this provision that judges can make use of any evidence in order to ascertain the truth. The judge thus analyses the evidence and then assesses whether it breaches any law to consider it admissible. The

[1191] Supreme No. 50/2011

way in which judges reach their decisions is also taken into account by other judges and thus aids them with identifying reliable sources. Judges have to reach truthful and fair decisions and they have to be therefore provided with evidence which confirms that it is right to convict the accused.

Furthermore, Article 179 of the Criminal Procedure Law provides that *"the court may of its own accord, during the examination of the case, order the producing of any evidence deemed necessary to reveal the truth."* In an unpublished Federal Criminal court case[1192], it was observed that the judge is obligated to study the evidence in order to identify whether it confirms that the accused is guilty of the offence. Furthermore, when the evidence is called into doubt, then the judge has to duly consider this.[1193]

At present, Article 5 of the Criminal Procedure Law states that the office of public prosecution is a branch of the judiciary and is responsible for investigating crime and bringing charges. It also falls on the public prosecutor to bring proceedings.[1194] However, it not only falls on the prosecution to provide evidence and the court can order that particular evidence is disclosed.[1195] The UAE Supreme Court has also affirmed that judges can look for evidence in order to establish facts.[1196] Yet it does not fall on the accused to provide evidence to show that s/he is innocent, but instead this is the task of the prosecutor. However, Article 2 of the Criminal Procedure Law allows the accused to

[1192] Supreme No. 10/2011
[1193] UAE Federal Criminal Case, Supreme No. 211/200
[1194] Article 7 of the Criminal Procedure Law
[1195] Article 179 of the Criminal Procedure Law
[1196] UAE Federal Criminal Case, Supreme No. 75/2011

present his/her own evidence in order to challenge the case of the prosecution. In this context, Article 229(2) of the Criminal Procedure Law states that:

> *"the objection should result in reconsideration of the case regarding the opposing party/the claimant before the court which rendered the judgment in absentia and the opposer/opposing party should not be harmed by his objection and if the opposing party did not appear before the first hearing specified for considering his objection, the objection shall be considered as if it did not happen, and the objection by the opposing party to the judgment rendered in his absence shall not be accepted."*

In a 2012 Federal Supreme Court case,[1197] the accused was charged for offending the honour and insulting a victim under the relevant section of the Penal Code, Article 373 and pursuant to the Sharia. The Court of First Instance decided without the accused being present that he should be fined and referred the case to the civil division. The accused challenged the decision and the court convened again, but without the accused being present and found again against him. The accused appealed this decision out of time and the court therefore refused the appeal. It was held that a decision reached without the accused being present, despite an objection having been lodged, is invalid. Hence, a court cannot consider objections which have been filed without the person being in attendance. However, this is not the case when a person was notified that the hearing takes place, but does not attend. In such a case, an appeal has to be brought.

[1197] Supreme No. 165/2012

Accordingly, evidence is normally presented during court proceedings and this evidence is gathered during the investigation, interrogation, as well as at the hearing. Judges particularly rely on the oral presentation during the hearing. However, such an approach may not prove effective when complex technical evidence is presented, in the absence of judges receiving training on how to deal with electronic evidence and to distinguish which evidence should be considered admissible and not admissible and which evidence should be disclosed in order to protect the work of enforcement agents. In this context, it has also been proposed at the 5th International Cybercrimes Conference in Abu Dhabi in 2014 that "specialized prosecutions in cybercrimes should be established in both the federal and local courts."[1198] Also, the lack of guidance for law enforcement bodies on how to investigate cases with an e-crime element and to collect electronic evidence means that judges are not in a position to determine whether evidence is reliable. The discretion which is conferred on judges therefore appears misplaced in the digital age. Instead it would be better if evidence was deemed valid so long as standardised digital evidence collection procedures have been complied with and this has been clearly documented.

The UAE's approach is also very different to the UK's common law approach since the UK provisions are far more detailed[1199], as discussed in the previous chapter. Whilst the approach which the UAE employs in terms of criminal procedure may have been

[1198] ME-Newswire, Cybercrimes Conference recommends establishing specialized prosecutions in federal and local courts, Abu Dhabi, UAE, 5 April 2014 <http://www.me-newswire.net/news/cyber-crimes-conference-recommends-establishing-specialized-prosecutions-in-federal-and-local-courts/en> accessed 26th April 2016

[1199] OECD, *Global Forum on Transparency and Exchange of Information for Tax Purposes, Peer Review Report Phase 1, Legal and Regulatory Framework United Arab Emirates* (Paris, OECD 2012) 14

suitable for traditional crime, this is inadequate for the digital age. The lack of special procedural rules for electronic evidence could bring into disrepute the judiciary and undermine the rule of law and may affect the ability to guarantee a fair trial. This is because the way in which electronic evidence is gathered is very different from normal policing techniques.[1200] In case an investigator fails to manage the digital evidence adequately, it may be of no value in court and standard procedures for the evidence collection, as well as preservation should be adopted in order to ensure that the custody chain is well documented.[1201] It is therefore important that electronic evidence rules are developed, which provide guidance in terms of collecting, presenting and preserving evidence and additionally to formulate rules when electronic evidence has been obtained through different types of surveillance in order to regulate when this evidence can be disclosed to the other side and to spell out when enforcement agencies cannot rely on this type of evidence at all, e.g. because of entrapment. This is also important since the Sharia imposes a strict standard of proof in respect of criminal cases and when there is any doubt, this goes in favour of the accused.[1202] Normally, it has to be also demonstrated that the accused had the requisite *mens rea* in respect of the crime.

The absence of clear evidence rules and the problems which this can cause is illustrated by a 2013 Federal Supreme Court case.[1203] In this case, a criminal conviction was

[1200] J. S. Dempsey, L. S. Forst, *An Introduction to Policing* (18th ed, Boston, Cengage Learning 2016) 499
[1201] K. M. Hess, C. H. Orthmann, H. L. Cho, *Police Operations: Theory and Practice* (6th ed, Boston, Cenage Learning 2013) 375
[1202] B. Ong, Standards of proof: is persuading the judge the 'ultimate threshold'? (2010) 5(2) *Construction Law International*, 35-38, 35
[1203] Supreme No. 120/2013

challenged on the basis that Articles 216 of the Criminal Procedure Law had not been met in respect of a conviction for a violation of Article 11 of Federal Law No.2 of 2006 regarding information technology crimes control which provides that:

> *"Each person who uses the website or other means of information technology to illegally access credit card numbers or information or other electronic cards, shall be punished by imprisonment and a fine, and if his intention of such use is to obtain others' funds or the service of such cards, he shall be punished by imprisonment for a period of no less than six months and by fine or by either of the two above mentioned punishments, and the punishment shall be a period of no less than one year and a fine of no less than thirty thousand dirham or by either of the two above mentioned punishments if concluded from such use to the seizure of others' funds for himself or others."*

Article 216 requires that the elements of the crime are satisfied and that there exists evidence to establish each element and inferences can only be drawn when there is sufficient evidence. Accordingly, it falls on the judge to prove and confirm all the facts and that the accused had the requisite intention, as defined by the legislation under which s/he is being charged. This has been interpreted to mean that the accused has to use the website or any other means of information technology to illegally access information or credit card numbers in order to seize the funds of others. In this case, the office of public prosecution had charged the appellant for stealing movable funds (credit

card) and used a webpage with the intention to access the credit card information and seized funds and paid for a traffic violation for his car. The defendant challenged the decision of the Court of First Instance on the basis that the elements of the crime had not been explained; the judgment was general and ambiguous; did not explain the circumstances of the alleged crime; and did not state on which evidence reliance was placed. Hence, the legal issue was whether it was insufficient for the First Instance Court to merely state that the accused had used the website and had accessed the credit card of the victim and seized money. It was argued that the court failed to identify how the elements of the crime had been carried out by the accused in order to establish his guilt and that as a result the decision was unsafe. The Supreme Court found that for a person to be convicted, each element of the crime has to be proven and has to be supported by evidence and inferences can only be drawn when the evidence clearly suggests this and there exists a sound basis for this. Accordingly, Article 216 of the Criminal Procedure Law requires that the presiding judge proves in his decision that the required acts are made out and that the accused had the requisite intention for the crime to be made out. The first instance court failed to explain how the appellant used the website or other means of information technology to access the credit card numbers. Moreover, the decision did not specify how the elements of the crime had been met. For this reason, it was held that the conviction should be overturned. Similar arguments can be made in respect of the other offences stipulated in Federal Law No.2 of 2006 and which may enable cyber criminals to escape their just punishment. The decision therefore highlights that the legislator has omitted to specify procedures designed to assist with evidencing digital crime. This is despite the fact that Articles 22 to 29 Arab

Convention on Combating Information Technology Offences require that state parties adopt procedural provisions for cybercrime offences.

Whilst Part III of the Criminal Procedure Law spells out the procedures which have to be followed during an investigation, these procedures are too basic for the digital age. Chapter IV allows the police to carry out searches[1204] and to seize[1205] evidence and these searches and seizures have to be overseen by a prosecutor. Yet the way in which this has been stipulated is outdated for the digital realm. For example, Article 75 of the Criminal Procedure Law provides that when a crime is suspected, enforcement officers can search his/her office or home and when evidence is found in respect of the crime, this has to be seized. However, it is insufficient to search an office or home, but for example, service providers must be obligated to furnish information. Article 30 of the Criminal Procedure Law also illustrates that the provisions are too rudimentary:

> *"the judicial police shall inquire about crimes, search for their perpetrators and collect the necessary information and evidence for investigation and indictment."*

Evidence, which has been confiscated, has to be placed in a sealed container and must be sent to the forensic laboratory. It is therefore important to reform these provisions, also in order to ensure that they are aligned, with the Arab Convention on Combating Information Technology Offences. The way in which the process of investigation is

[1204] Articles 51-59 of the Criminal Procedure Law
[1205] Articles 60-61 of the Criminal Procedure Law

explained must be updated,[1206] as well as how general evidence and information should be gathered about a crime.[1207] As highlighted by the analysis of the UK legal framework, the topic of surveillance and interception must be addressed, which currently has not been done. The Arab Convention on Combating Information Technology Offences also mandates this, for instance, Article 29 calls for 'interception of content information.' The requirement to follow documentation procedures[1208] must be fleshed out, as the UK has done[1209], for instance, through a guide for digital evidence which also details the procedures which managers of e-crime investigations must follow.

Without such steps being taken it is unlikely that the prosecution can demonstrate that digital evidence is admissible. It will be difficult to show that the evidence is legitimate and judicial since the procedures have not been clarified to deem digital evidence admissible. Instead, a search only requires that a search warrant has be obtained, as made clear by Article 53, which provides:

> *"The judicial police officer may not inspect the dwelling of the accused without a written authorization from the public prosecution unless the crime is in the process of being committed and there are strong indications that the*

[1206] Chapter 1 of the Criminal Procedure Law
[1207] Article 30 of the Criminal Procedure Law
[1208] Article 36 of the Criminal Procedure Law
[1209] The Association of Chief Police Officers Good Practice Guide for Digital Evidence 2012, <http://www.acpo.police.uk/documents/crime/2011/201110-cba-digital-evidence-v5.pdf> accessed 2 May 2014; the Association of Chief Police Officers Good Practice Guide for Computer-Based Electronic Evidence, <http://www.7safe.com/electronic_evidence/ACPO_guidelines_computer_evidence.pdf> 2 May 2014; the Association of Chief Police Officers Good Practice Guide for Managers of e-Crime Investigation, <http://www.acpo.police.uk/documents/crime/2011/201103CRIECI14.pdf> accessed 2 May 2014

accused is hiding in his house, objects or papers which may lead to the truth."

A search warrant can be issued when a crime has been committed; it is serious; and the act constitutes a criminal offence as stipulated in Article 72. However, no searches can be conducted without a crime having been committed. Such an approach is problematic in the digital age where a proactive policing approach is important.[1210]

There are three types of crimes and a search warrant can only be granted for what are felonies, but not in respect of misdemeanours. Article 28 makes clear that a felony is an offence which attracts at least three years' imprisonment or more. Article 29 explains that a misdemeanour is an offence which attracts between one week and up to three years or a fine which does not exceed AED 1,000. In contrast, a petty misdemeanour only attracts imprisonment between one and ten days or a fine.[1211] However, the limitation to only grant a search warrant for felonies may be too restrictive to adequately police the digital space.

Furthermore, no details are provided about what should be seized, but instead a broad-brush approach has been adopted by the Criminal Procedure Law, Article 61 which states that:

[1210] T. J. Holt, A. M. Bossler, *Cybercrime in Progress: Theory and Prevention of Technology-enabled Offenses* (Abingdon, Routledge 2016) 124
[1211] Article 30 of the Criminal Procedure Law

> *"the judicial police officers have to sequestrate the objects which may have been used in the perpetration of the crime, resulted therefrom or if the crime has been committed thereon; in addition to whatever may lead to the truth in the matter."*

Yet when evidence is obtained from a network or a cloud, no tangible property is seized, and it is unclear whether this provision, despite its wide ambit in terms of what can be seized, is broad enough. The scope of what can be search and seized is set out by the search warrant, but such an approach is too limiting for the digital world in the absence of powers which permit surveillance.

Moreover, as only evidence can be searched and seized, which has been *"used in the perpetration of the crime"*[1212] issues may also arise since it is unclear whether this also includes, e.g. networks employed to facilitate the crime. Another problem is the way in which Article 51 is worded, as an inspection is defined as *"the search of the body, clothes or luggage for any trace or things related to the crime or required for the investigation."* This is clearly an outdated definition, which is insufficient to cover the digital realm. Yet it may be argued that a broad construction of what can be deemed *"things"* ensures that this also extends to digital devices, networks, software, etc. Nonetheless, it would be better to revise this provision.

The public prosecutor is in charge of the search warrant, though s/he can pass it to the officer in charge of the investigation in accordance with Article 33 of the Criminal

[1212] Article 61 of the Criminal Procedure Law

Procedure Law. When the public prosecutor does not personally execute the search warrant, those who have been provided with it, have to follow the exact steps detailed by the prosecutor on the search warrant. Yet the Criminal Procedure Law does not contain any provisions which require that only officers, who are adequately trained, conduct searches and seizures of electronic evidence. This may call into doubt the evidence and should be addressed.

Article 53 of the Criminal Procedure Law permits the public prosecutor to determine whether a place should be searched on or off-site. However, this provision is too narrow to confer powers to continuously monitor networks through back entrances made available by the private sector, e.g. social media, such as Facebook. This is also the case because of the requirement that a crime has to have already taken place.

Nonetheless, a search warrant is not always required, and the Criminal Procedure Law also permits surveillance without a search warrant. Article 54 of the Criminal Procedure Law states that:

> *"the judicial police officer, even in cases other than a crime that is in the process of being committed, may inspect dwellings of persons put under surveillance, either according to a provision of law or a decision by a judge, should there be strong indications that they may be suspected of perpetrating a felony or a misdemeanour."*

The way the provision is phrased is problematic since surveillance should be much wider than inspecting dwellings of persons when the crime is currently being committed. Most transactions are carried out through digital devices and over networks and interpreting this section to include surveillance of social media activities of a person, his/her internet activities and searches, etc. may strain the language of this section too much. It would therefore be better to revise this provision altogether or at least to complement it. This is also important in light of the fact that the police conduct internet surveillance and similarly, the Department of Anti-Electronic Crimes and Abu Dhabi's State Security Apparatus have also established a specialised unit in order to conduct surveillance; however, this activity is currently unregulated and has not been put on a statutory footing.[1213]

Such an approach is also warranted, as currently *"members of the public authority (i.e. law enforcement authorities such as police) may not enter into any place of residence except under the circumstances specified in this law or in case of a request for assistance from inside or under a serious threat on life or property".*[1214] As cybercrime does not normally involve a serious threat to life or property from inside a residence, investigative powers of the enforcement agencies are severely limited by the narrow scope of the Criminal Procedure Law, which is still focused on traditional crimes.

[1213] A. Al Neyadi, A. Al Kaabi, L. al Kabi, M. Al Ghufli, M. Al Sahmsi, M. Khan, 'Internet Governance & Cybercrimes in UAE (2015) 4(11) *International Journal of Scientific & Technology Research*, 350-357, 352

[1214] Article 3 of the Criminal Procedure Law

Moreover, a search warrant is also not needed when "*the crime is in the process of being committed and there are strong indications that the accused is hiding in his house objects or papers which may lead to the truth."*[1215] However, the issue with this provision is also that it does not permit a pro-active policing approach. Again, the way in which this section is worded is rather outdated, as only a purposive approach permits that intangibles fall within the scope of this provision.

The current Criminal Procedure Law does not address electronic evidence sufficiently and should be substantially revised and complemented.

4.3 Summary

The UAE's e-crime framework is expansive; as the government has launched many different initiatives, which are also coordinated by the NESA. The replacement of Federal Law No.2 of 2006 on combating cybercrime with the new Federal Law No. 5 of 2012 concerning Combating Information Technology Crimes has been an important step to improve the legislative e-crime regime. However, whilst the UAE has recognised the importance of data protection for the DIFC, the same cannot be said for the rest of the UAE. Nonetheless, Federal Law No. 5 of 2012 increases privacy protection by outlawing various activities, though this approach is insufficient to achieve comprehensive data protection. Data protection can be an important tool against cyber-security incidents since businesses can be required to only store as much data as is necessary. As a result, cyber criminals can then obtain less data in case they succeed

[1215] Article 53 of the Criminal Procedure Law

with an attack. Data protection principles can also act as a barrier of defence against cybercrime.

The scope of the offences is also very broad, and it would be useful to issue guidelines. This may also prevent that unnecessary legal challenges are brought. Similarly, it is important to clarify whether the cybercrime offences have extra-territorial effect in light of the provisions of the penal code, despite the cybercrime law suggesting that this is limited to cyber attacks directed against emanations of the state. In this context, it is also important that public prosecutors receive more guidance. Additionally, the government should try and enter into extradition treaties with other countries, as otherwise the extra-territorial provisions may not be enforceable.

One of the most pressing issues is to ensure that the surveillance activities by enforcement agents are put on a statutory footing and that formal powers are spelled out. Otherwise, the UAE risks being in breach of international law, as surveillance breaches the right to privacy, which is also guaranteed by the UAE constitution. Federal Law No. 5 of 2012 concerning Combating Information Technology Crimes also contains various provisions which are aimed at protecting privacy. Yet the thorny issue of how to balance surveillance powers and privacy rights has not been addressed. The issue is that surveillance powers can be abused, and it is therefore important that legal safeguards are developed. Just like search warrants have to be issued, it is important that a debate is started about how the surveillance powers can be kept in check in a way which accords with fundamental values, such as the rule of law.

There are some other gaps within the legislative provisions. At present, Federal Law No. 5 of 2012 concerning Combating Information Technology Crimes fails to address the issue of attacks against critical national infrastructure. In light of the UAE adopting a smart grid and building its first nuclear power plant and having many oil installations, it is therefore important that an appropriate offence is added to the existing ones and which should be added to the category of offences which deal with state and political security.

The UAE should also consider whether an explicit legal requirement should be imposed on certain sectors to notify security breaches to the authorities. This would create an information loop and could ensure that precautions are taken against particular attacks. Closer cooperation with the private sector is also important and the NESA should work on signing agreements with the private sector, particularly social media companies. Also, as Intellectual Properties (IP) have assumed much more importance in an information society, the legislator should also study whether a specific offence should be added to Federal Law No. 5 of 2012 in order to criminalise serious IP violations and whether enforcement agencies should be equipped with more powers to investigate serious cases of IP violations. The government should also continue to lobby other Middle Eastern states, so that the procedures for the Arab Convention on Combating Information Technology Offences are agreed and co-operation is further increased based on common standards and mutually agreed offences.

Another pressing issue, which should be addressed by the legislator, is to update the Criminal Procedure Law Federal Law No. 35 of 1992. Only specialised police officers, who are trained in recovering digital evidence, should collect digital evidence. Equally, public prosecutors and judges should receive training and they could then be responsible for bringing cybercrime prosecutions and hearing cybercrime cases.

At present, the provisions are unclear in respect of the gathering of evidence which is stored on a cloud or network, as the way in which certain provisions are worded relates to traditional crime and tangible property, as opposed to intangible property. The way in which an inspection is defined also highlights that the law is outdated. New provisions have to be adopted for digital surveillance, including authorisation procedures, similar to the search warrant regime, so that there is sufficient oversight. The investigative powers should also be broadened to include new powers to gather data and to require internet service providers to store search records. Providers of encryption services should also be legally mandated to hand over encryption keys to enforcement agencies when this is needed to investigate a cybercrime.

Chapter Five: Understanding How to Strengthen E-Crime Legislation in the UAE Through Interviews with Senior E-Crime Experts

5. Introduction

As explained in Chapter Two, whilst the doctrinal black letter law method constitutes a considerable part of the thesis, a mixed methods approach was adopted overall. In the preceding chapters doctrinal legal analysis has been used to analyse the formulation of legislation, regulations and statutes related to e-crime in the UK, the EU and the UAE. However, legal scholarship acknowledges that doctrinal analysis implicitly incorporates external factors, such as when the historical or social context of legislation is evaluated in order to better comprehend and interpret specific legal rulings.[1216] Taking this viewpoint into account, the research explicitly supplements the black letter law method with empirical data from the UAE for an increased understanding of the effectiveness of the legislation under discussion and to examine the extent to which it is being complied with. As explained in Chapter Two, this is a mixed methods strategy allowing for triangulation, it is used as a vehicle to illuminate and capture a more complete and contextual portrayal of the research phenomenon and to examine it from multiple dimensions and perspectives.[1217]

[1216] P. Chynoweth, 'Legal research', *Advanced Research Methods in the Built Environment* (Oxford, Wiley-Blackwell, 2008) 28-38

[1217] T. D. Jick, 'Mixing Qualitative and Quantitative Methods: Triangulation in Action' (1979) 24 (4) *Qualitative Methodology* 602-611

The chapter presents the findings from the in-depth interviews with the most senior experts in the UAE from the police, the office of prosecution, the judiciary, the Telecommunications Regulatory Authority and Interpol. Five interviews were conducted. After the fifth interview, no new data was obtained, and data saturation was therefore reached.[1218] The themes were exhausted and a varied data set was obtained.[1219] The research participants were all given a consent form asking them to agree to take part in the research. A flexible guided interview approach was adopted, which enabled the researcher to respond to unanticipated replies.[1220] The researcher thus used a schedule, but this only served as a guide since it was more important to have a good rapport in order to probe further and identify the interviewees particular concerns.[1221] A content analysis was undertaken to analyse the data and themes, patterns and categories were identified, and the data was reduced to explain its meaning.[1222] The text was closely read and interpreted in light of the context and codes and clusters were created, as explained in Chapter 2.[1223]

[1218] D. E. Gray, *Doing Research in the Real World* (London, SAGE Publications Ltd 2014) 147; P. I. Fusch, L. R. Ness, Are We There Yet? Data Saturation in Qualitative Research, 9(1) *The Qualitative Report* 2015, 1408-1416, 1409
[1219] G. Guest, A. Bunce, L. Johnson, How Many Interviews Are Enough?: An Experiment with Data Saturation and Variability, 18 *Field Methods* 2006, 59-82, 65
[1220] J. Willis, *Qualitative Research Methods in Education and Educational Technology* (Charlotte, Information Age Publishing Inc 2008) 205
[1221] S. J. Yates, *Doing Social Science Research* (London, SAGE 2003) 165
[1222] L. M. Given, *The Sage Encyclopedia of Qualitative Research Methods, Volume 2* (London, SAGE 2008) 120
[1223] Ibid

5.1 Discussion and Analysis of The Qualitative Interviews

The interviews provided comprehensive and in-depth insights about the effectiveness of UAE's legislative framework to combat e-crime. This is particularly useful to understand more fully the research phenomenon, especially in light of the relevant literature.

5.1.1 Key Findings and the Relevant Literature

The interviewees generally agreed that the UAE had taken important steps to secure the digital realm by passing Federal Law No.2 of 2006 on the Prevention of Information Technology Crimes, as well as Federal Law No. 5 of 2012 on Combating Cybercrimes. It was thought that the listed cybercrime offences were expansive and could be interpreted to cover most crimes, together with other offences in the Penal Code. Moreover, the recent reforms to the UAE Penal Code by virtue of Federal Law No.7 of 2016, which impose stricter penalties and higher fines, further heighten deterrence.[1224] This is because these provisions can also be applied to the digital realm. Nonetheless, it was recommended that the e-crime law is updated and important improvement recommendations were made. As expressed here by Interviewee A:

> [*T*]*echnology is in continuous development and so are crimes, therefore laws should be re-drafted, discussed and reviewed every now and then, due to the development of crimes which may have not been covered by the previous laws.* [*T*]*echnology is in a continuous process of development that requires laws to be up to date, so that the law does not remain static...*

[1224] H. Dajani, Sweeping reforms to UAE penal code include harsher penalties and up to Dh1m in fines, The National, 25 October 2016 <http://www.thenational.ae/uae/sweeping-reforms-to-uae-penal-code-include-harsher-penalties-and-up-to-dh1m-in-fines> accessed 15th February 2017

International co-operation was deemed one of the pressing priorities in order to bring cyber criminals to justice. It was pointed out that cybercrimes were very often cross-border crimes. However, presently co-operation, including through diplomatic channels, was considered a challenge for a multitude of reasons, including cybercrime laws in other countries. It was explained that issues can arise, for instance, when the accused is in a European country and the service used for committing the crime is in the US and the victim is in the UAE. Three sets of legislations govern this case. Without an international cybercrime treaty, these cases are difficult to resolve.[1225] However, to date conclusion of a UN-based cybercrime treaty has been deferred, as evidenced by a recent draft resolution adopted at a meeting by the Commission on Crime Prevention and Criminal Justice in April 2013.[1226] The resolution states that member states should "continue to consider...ways and means to strengthen international cooperation in combating cybercrime."[1227] Yet the Arab Convention on Combating Information Technology Offences 2010 ensures that there is at least some cooperation amongst Arab League nations.[1228] However, it was observed that cooperation amongst the Arab countries has to be strengthened, so that it is on par with the cooperation which exists in Europe as a result of the Council of Europe Convention on Cybercrime 2001.

[1225] J. Clough, *Principles of Cybercrime* (2nd ed, Cambridge, Cambridge University Press 2015) 25
[1226] Commission on Crime Prevention and Criminal Justice, *Draft resolution: strengthening international cooperation to combat cybercrime*, UN ESCOR, 22nd sess., Agenda Item 7, UN Doc E/CN.15/2013/L.14 (2 April 2013) 2, Article 2; J. Clough, *Principles of Cybercrime* (2nd ed, Cambridge, Cambridge University Press 2015) 25
[1227] Commission on Crime Prevention and Criminal Justice, *Draft resolution: strengthening international cooperation to combat cybercrime*, UN ESCOR, 22nd sess., Agenda Item 7, UN Doc E/CN.15/2013/L.14 (2 April 2013) 2, Article 2; J. Clough, *Principles of Cybercrime* (2nd ed, Cambridge, Cambridge University Press 2015) 25
[1228] Judge Stein Schjolberg, A presentation at the Europol-INTERPOL Cybercrime Conference, Europol, The Hague, 24-25 September 2013, 1-15, 3 <http://www.cybercrimelaw.net/documents/Europol-INTERPOL.pdf> accessed 15th February 2017

Furthermore, whilst cooperation is also facilitated, e.g. through organisations, such as Interpol, countries are not required to provide assistance when this is requested. Disagreement by countries over what should be considered a cybercrime made cooperation difficult. As explained here by Interviewee B:

> "[*C*]*ybercrime is a cross-border crime and this a great challenge... each country has its own law which differs from that of other countries, a matter which leads to disagreement over what is considered to be a crime...*"

The interviewees therefore emphasised that international and regional efforts are paramount and have to be pursued in tandem with national strategies in order to effectively combat cybercrime. On this point Interviewee A stated:

> *"Why not work on an international agreement under the umbrella of the United Nations to address cybercrimes similar to the European Agreement."*

All of the interviewees stressed that the most pressing matter for the UAE was to enact a law which regulates the processes and procedures for e-crime investigations and prosecutions, including in respect of preventative measures. It was explained that there is no law which details how cybercrime should be dealt with. Federal Law No. 35 of 1992 concerning the Criminal Procedural Law was deemed inadequate, as it only addresses crimes in general. Aljneibi also shares this view and states that the current Criminal Procedures Law, whilst being a useful framework, cannot be extended to electronic evidence procedures, as more specific regulations are required for electronic

searches, seizures, examination and retention.[1229] The interviewees were concerned that without enactment of such a law, this legislative gap would enable criminals to continue escaping punishment.

Moreover, it was generally thought that surveillance is important, but that it has to be strictly controlled in order to avoid that the privacy of individuals was unduly violated. This accords with the literature which also makes clear that surveillance methods have to be regulated by law.[1230] The lack of clear laws to regulate surveillance, data retention, decryption requests, equipment interferences and related law enforcement powers was thus perceived as another pressing issue. It was recommended by the interviewees that these powers should be clearly detailed in a statute with appropriate controls. Banning encryption was not considered a wise strategy and all the interviewees were against a ban. The above factors were summed up by Interviewee B in this way:

> *"In my opinion, the acquisition of data/information about a person or entity should be organized by law, as well as decryption/ decoding, because without legal authorization such actions may not be taken by control bodies. Regarding its importance, it sure is of great importance in the detection of crimes, but this should be done taking into consideration privacy, as it is important to detect crimes of course, however, this should be done without committing another crime which infringes privacy; my knowledge of the*

[1229] K. A. Aljneibi, The Regulation of Electronic Evidence in the United Arab Emirates: Current Limitations and Proposals for Reform, PhD Thesis, February 2014, 1-326, 194 <http://e.bangor.ac.uk/4992/1/Aljneibi%20khaled%20thesis.pdf> accessed 15th February 2017

[1230] N. Taylor, Policing, privacy and proportionality, *European Human Rights Law Review* 2003, 86-100, 91

email of the accused does not mean that I have to penetrate/intrude such email without obtaining permission from the competent authorities... As I have mentioned earlier, I agree with encryption and I am against the prevention of encryption, but this should be in accordance with legal procedures."

The interviewees also thought that the digital age required special data protection laws, as this was considered "to prevent penetrations/breakthroughs", as observed by interviewee A. Hence, data protection regulation was perceived as a means to safeguard individuals against cybercrime. Similarly, Wong observes that data protection laws are part of a holistic strategy to create cyberdefence and resilience.[1231] Such laws are also essential in an age of preventative policing where the "professional law enforcement model of policing...[has shifted] to cyber policing" which is inherently more proactive.[1232] Otherwise there is the risk that "notions of criminal justice" and the "democratic balance of power" become distorted.[1233] The adoption of measures to safeguard the right to privacy and data protection which curtail policing powers and result in technological transparency thus also promote accountability, fairness, proportionality and equality.[1234] Similarly, evidence rules, which prevent admission of

[1231] R. Wong, *Data Security Breaches and Privacy in Europe* (London, Springer 2013) 36
[1232] N. Kozlovski, A Paradigm Shift in Online Policing - Designing Accountable Policing, Yale Law School, 2005, 1-22, 20-21 <https://crypto.stanford.edu/portia/papers/Kozlovski.pdf> accessed 1st March 2017
[1233] Ibid, 21
[1234] Ibid

intercept material, are important to ensure that due process standards are embedded within the law.

5.1.2 Legislation for Cybercrime Offences

In comparison to other countries in the region, the UAE was one of the first countries in the Middle East and North Africa to criminalise IT crimes through the passing of Law No. 2 of 2006.[1235] It was pointed out that prior to 2006, the Federal Law No. 3 of 2003 on Telecom Law had to be relied upon, alongside the Penal Code, in order to prosecute cyber criminals. However, it became increasingly clear that this law was insufficient to safeguard UAE society from the threats of cybercrime. The majority of interviewees thought that the cybercrime laws were good. The six-year time period after which the 2006 law was reviewed was deemed an appropriate timeframe. Nevertheless, 2018 will mark the end of the current six-year time period. All of the interviewees stressed that the existing legislation should be reviewed in light of rapidly advancing technology and new criminal behavioural patterns. This aspect was elucidated by Interviewee E in this way:

> "[*T*]*he problem lies with failure by the law to cope with the pace of technological development and the behavioural patterns of the criminal, so we find that the first law related to cybercrimes was issued in 2006 and then replaced by another law issued in 2012, and during these six years the patterns of crimes have changed and new ones have appeared, and since the*

[1235] N. Kshetri, *The Global Cybercrime Industry: Economic, Institutional and Strategic Perspectives* (London, Springer 2010) 148

issuance of the law four years back, new behavioural patterns have emerged which may not be legally characterized pursuant to the law, therefore, the law needs to be continuously amended."

Consequently, the existing provisions should be continuously reviewed, discussed and amended. Otherwise, the risk is that the law will not keep pace and there will be a legislative gap which allows criminals to escape their just punishment. In this context, Interviewee A noted:

"I cannot say that there are no shortcomings in the legal provisions. This is because new developments in IT occur on a daily basis."

The literature also confirms that cybercrime laws have to be regularly updated.[1236] Hence, the challenge for the UAE is not to have time elapse between identifying possible abuses through technologies and changing its cybercrime legislation, so that the law remains fit for purpose.[1237] This adjustment process necessitates recognising how new technology is being abused; identifying gaps within the legal provisions and drafting new laws, ideally in line with international strategies and standards.[1238] However, in this context it is also important to bear in mind that traditional offences can be extended, as these are technology neutral.[1239] Hence, the fact that the crime has been

[1236] R. Broadhurst, P. Grabosky, *Cyber-Crime: The Challenge in Asia* (Hong Kong, Hong Kong University Press 2005) 145
[1237] M. N. Sirohi, *Transformational Dimensions of Cybercrime* (Delhi, Alpha Editions 2015) 50-51
[1238] Ibid
[1239] UK House of Commons: Science and Technology Committee, *Malware and cybercrime: Twelfth Report of Session 2010-12, HC 1537* (London, TSO Shop 2012) 21

committed through the digital environment does not mean that no charges can be pursued.[1240] As pointed out by Interviewee D:

> *"Federal No. 5 of 2012 is flexible and can also be addressed to new crimes…Public prosecutors and judges must be qualified and have extensive experience in characterising crime."*

As discussed in Chapter one, in the UK cyber criminals can also not just be charged under the Computer Misuse Act 1990. Instead other legislation can be used to prosecute cyber criminals, for instance, the Obscene Publications Act 1959 and 1964 deals with electronic pornographic offences and the Sexual Offences Act 2003 deals with online and offline sexual grooming.[1241] It would therefore be useful if public prosecutors and judges who specialise in cybercrime received training in evoking existing penal provisions for crimes which can be committed online. This will avoid the problem of criminals escaping punishment for lack of an adequate characterisation of the particular offence, which was identified as a problem by the interviewees.

Whilst it is possible to apply traditional offences to the digital realm, some of the interviewees argued that the offences in Federal Law No. 5 of 2012 should be extended and/or further clarified. They explained that that at present certain crimes are only indirectly addressed by the legislation. For instance, there is no provision contained in the law to cover situations where a person impersonates another person on social media

[1240] Ibid

[1241] J. X. Kelly, Computer Misuse Overview, JISC Legal Information, 2007 <http://www.jisclegal.ac.uk/LegalAreas/ComputerMisuse/ComputerMisuseOverview.aspx> accessed 17 June 2014

i.e. establishes an account in the name of another person, including a public figure. Whilst these crimes can nevertheless be prosecuted by placing reliance on the Penal Code and other cybercrime provisions, it was noted that the issue is that this crime cannot be characterised. It was therefore considered better if a provision was enacted which proscribes fraudulent online impersonation. Otherwise, judges are afforded broad discretion to convict those who are accused of these crimes. Whilst this discretion is curtailed by the oversight by the Court of Cassation, the law will be improved if this was addressed in a specific provision. This will also enhance legal certainty and thus promote the rule of law.[1242]

Moreover, it was pointed out that the law omits to specify the meaning of privacy, despite Article 21 criminalising the invasion of privacy through use of a computer network and/or electronic information or any information technology means through, for example, eavesdropping, photographing others or publishing news. This was considered a serious problem by the interviewees since those who had been charged for taking pictures of persons and thereby abusing their privacy had all been acquitted. This is because Article 31 of the UAE Constitution cannot be extended to these types of situations, as reference is only made to "freedom of communication by post, telegraph or other means of communication and the secrecy thereof shall be guaranteed in accordance with the law." The other provision which indirectly safeguards privacy is Article 379 of the Penal Code.[1243] However, this provision can also not be applied to this

[1242] P. H. Neuhaus, Legal Certainty versus Equity in the Conflict of Laws, 28(4) *Law and Contemporary Problems* 1963, 795-807, 795

[1243] Article 379 of the Penal Code states "…Any individual who, by reason of his profession, craft, circumstance or art is entrusted with a secret and who discloses it in cases other than those permitted by

new context, as it only covers circumstances where a person discloses secrets without the individual with the secret agreeing to this. Accordingly, the legislator should clarify what amounts to a privacy infringement.

In this context, it would be important to additionally clarify Article 2(3) of Federal Law No. 5 of 2012 Concerning Combating Information Technology Crimes which intends to confer data protection in respect of "personal data" and "personal information objects." This is because the law criminalises the commission of various acts against such data in Article 2(2), for instance, deletion, disclosure, alteration or publication. Moreover, at present such data is not protected against the acts listed in Article 2(1), as Article 2(3) only spells out punishment for acts done in respect of personal data and personal information objects "mentioned in paragraph (2) of this Article." This unduly narrows the scope of protection for personal data and personal information objects. It would be better if the scope was extended to also cover the acts in Article 2(1) i.e. to access personal data and personal information on "a website, an electronic information system, computer network or information technology without authorization or in excess of authorization or unlawfully." Furthermore, currently the law only stipulates that cyber criminals can be fined or imprisoned, but omits to afford remedies to victims. It would be better if those who have suffered reputational or psychological damage could seek damages.[1244] The interviewees therefore recommended that either Federal Law No. 5 of 2012 should define the concept of private life or that a privacy and data protection law

---

the law, or who uses it for his own advantage or another person's advantage, shall be [punished] unless the individual to whom the secret pertains has consented that it be disclosed or used."

[1244] Information Resources Management Association, *Cybercrime: Concepts, Methodologies, Tools and Applications* (Hershey, Information Science Publishing 2012) 1358

should be enacted. Manoharan and Holzer also observe that the "UAE lacks an online privacy law."[1245]

One of the interviewees stressed that Federal Law No. 5 of 2012 needs to be re-drafted, as various articles overlap. The interviewee explained that this caused confusion when investigations were conducted and made it difficult to characterise the crime at trial. For example, Article 2 of Federal Law No. 5 of 2012 addresses more than one behavioural pattern, namely access without permit, violating the limits of the permit and staying at an unauthorised location. Several other provisions include more than one behavioural pattern. This makes it difficult to interpret the provisions, especially when the acts are similar, for instance, as is the case with Articles 12 and 13. Article 12 deals with obtaining bank data, as Article 13 does, but it was pointed out that the latter provision has been interpreted differently. Article 12 criminalises "gain[ing] access, without legal right, to credit or electronic card numbers...." for the purposes of "us[ing[these data and numbers to take over the funds of others..." Similarly, Article 13 criminalises "forg[ing], counterfeit[ing] or reproduc[ing] a credit card or debit card...." [and] (2) us[ing it], without authorization to obtain....funds.." Whilst an analysis of these provisions shows that there is a difference between using someone's credit card and making a copy of it and the latter act warrants more serious punishment, future legislation should be clearly drafted. This is also important, as it was noted that the terminology and vocabulary employed by the legislative provisions could be clearer. Otherwise, the problem will persist that many accused escape their punishments because of overlapping provisions.

[1245] A. Manoharan, M. Holzer, *Active Citizen Participation in E-Government: A Global Perspective* (Hershey, Information Science Reference 2012) 469

It was suggested that the law should not only list examples of incriminating, but also non-incriminating acts to provide more guidance. In the alternative, it could become a standard practice to issue explanatory notes whenever federal laws are passed, as the UK does.[1246] On this issue, Interviewee A stated:

> *"Over time, the Supreme Court may also issue judicial principles, so that the provisions are further explained and interpreted. This will help with applying the provisions to new IT crimes. Whilst such principles are not binding, as in jurisdictions, such as the UK, they are explanatory."*

One of the interviewees explained that under Law No. 2 of 2006, the punishment for cyber criminals who targeted critical infrastructure was 10,000AED (around £2,200), whereas under Federal Law No. 5 of 2012, offenders can also be imprisoned. Additionally, offenders can be charged for felonies, depending on the magnitude of the act. However, attacks on critical infrastructure are not specifically addressed by Federal Law No. 5 of 2012. Whilst the law lists various offences, it appears difficult to apply them to situations where computers are impaired in order to cause serious damage or the risk of serious damage, e.g. to the soon completed nuclear power station in the UAE or oil installations.[1247] For instance, the provision which deals with terrorism (Article 26) simply outlaws "establishing, managing or running a website or publishing

[1246] For instance, see the Serious Crime Bill, Explanatory Notes, 2014, 1-85, 2 <http://www.publications.parliament.uk/pa/bills/lbill/2014-2015/0001/en/15001en.pdf> accessed 20th January 2015

[1247] S. Hinson, Nuclear power on schedule in the United Arab Emirates, Weinberg Foundation, 10 January 2017 <http://www.the-weinberg-foundation.org/2017/01/10/nuclear-power-on-schedule-in-the-united-arab-emirates/> accessed 28th February 2017

information...for the interest of a terrorist group...” Whilst Article 44 makes clear that Articles 4, 24, 26, 28, 29, 30 and 38 also constitute crimes against state security, an analysis of these provisions shows that these do not cover attacks against critical infrastructure. Also, critical infrastructure may be privately owned, so that a provision which only criminalises causing serious damage or risk of serious damage to state-owned critical infrastructure would be insufficient. It is therefore very important that an additional provision is added which criminalises the impairment of a computer in order to cause or to cause risk of serious damage to UAE’s national security, the economy, the environment or human welfare, as the UK has done by virtue of section 3ZA of the Computer Misuse Act 1990, as discussed in Chapter 1. This is also imperative in light of many cyber criminals trying to attack critical infrastructure and critical services in the UAE.[1248] In this context, Maj Almarashda states that “[t]he protection of the critical national infrastructure involving oil, gas, water and electricity in the UAE is lagging. The result is this could cause major disturbances to key services.”[1249] Equally, Dr Saud Al Junaibi points out that the UAE’s capacity to utilise data detection systems to protect critical infrastructure could be further improved.[1250] Adoption of a specific legal provision, which punishes hackers who attack critical infrastructure, is therefore an important step to heighten cyber security, alongside other practical strategies and measures.

[1248] C. Malek, UAE needs better protection of critical infrastructure, The National, 19 November 2014 <http://www.thenational.ae/uae/technology/uae-needs-better-protection-of-critical-infrastructure> accessed 22nd August 2015

[1249] E. Samoglou, UAE researcher calls for more stringent cyber security, The National, 1 April 2015 <http://www.thenational.ae/uae/technology/uae-researcher-calls-for-more-stringent-cyber-security> accessed 24th February 2017

[1250] C. Malek, UAE needs better protection of critical infrastructure, The National, 19 November 2014 <http://www.thenational.ae/uae/technology/uae-needs-better-protection-of-critical-infrastructure> accessed 22nd August 2015

All of the interviewees agreed that one of the main challenges is that cyber criminals are often not located within the UAE. Several of the interviewees therefore suggested extending the scope of Article 47 of Federal Law No.5 of 2012. It was pointed out that Federal Law No.5 of 2012, Article 47 only confers extra-territorial jurisdiction in cases where cybercrime directly prejudices the interests of the state. In such an instance, a person can be prosecuted, even if the act was not committed in the UAE. However, this provision is an exception and can only be evoked when a person commits cybercrimes against the state. Nonetheless, it was stated that Federal Law No. 5 of 2012 is a marked improvement to Federal Law No. 2 of 2006, which did not contain such a provision. However, the scope of this provision is curtailed, as companies, e.g. private banks, cannot demand that cyber criminals are extradited. In contrast, in the UK extra-territorial jurisdiction is much more comprehensive, as extra-territorial jurisdiction can also be sought when the private sector is the victim of a cybercrime offence. Furthermore, those who live in the UK, but commit a cybercrime in another country, as well as UK nationals who reside abroad and who commit a cybercrime in the UK, fall under the jurisdiction when there is a significant link to a relevant jurisdiction.[1251] Also, UK nationals can be prosecuted when there is no significant link to the UK, so long as the offence is one in the country where the person resides.[1252]

The UK approach is beneficial for and promotes cooperation with other countries. As stressed by Interviewee D, the main problem with combating cybercrime is "lack of

[1251] Ss4-5 of the Computer Misuse Act 1990; Serious Crime Act 2015, Explanatory Notes, para.137 <http://www.legislation.gov.uk/ukpga/2015/9/notes> accessed 1st December 2015
[1252] S.5(1a) and (1B) of the Computer Misuse Act 1990

sufficient international coordination." However, at present Federal Law No. 5 of 2012 does not promote international cooperation, as enforcement agents cannot rely on the UAE to assert "legal power beyond its territorial borders" in order to ensure that cyber criminals are brought to justice.[1253] The UAE's stance towards combating cybercrime is therefore less aggressive than that of the UK. Yet as cybercrime has not yet been regulated at the international level, this may be warranted. In this context, some of the interviews also observed that other countries may not recognise the UAE asserting jurisdiction over nationals in their jurisdiction, Interviewee A said:

> *"This raises the question whether other countries will give up their territorial jurisdiction and allow other countries to extend theirs."*

The application of domestic laws to activities which are unrelated to the UAE territory may be deemed objectionable by other countries, especially when UAE law does not transpose international law.[1254] For instance, some of the interviewees explained that certain offences are not deemed crimes in other countries. Interviewee D furnished the following example:

> *"The law in the United Arab Emirates, for instance, punishes taking a picture of a person without his/ her permission at a public place and in some countries this is not considered a crime being taken at a public place….We*

[1253] A. J. Colangelo, What is extraterritorial jurisdiction? 99 *Cornell Law Review* 2014, 1303-1352, 1303
[1254] Ibid, 1332-1333

also have freedom of the press, but within the limits of not insulting and defaming others, while in some countries this is considered permissible."

Nonetheless, it would be better if the law reassured other countries that criminals can be pursued for acts which constitute an offence under the law of the country in which it occurred, so long as it corresponds with one of the offences set out in Federal Law No. 5 of 2012.

At present, extra-territorial jurisdiction cannot only be evoked pursuant to Article 47 of Federal Law No. 5 of 2012, but also by virtue of Federal Law No. 3 of 1987 (the Penal Code), as explained by some of the interviewees. Article 23 of the Penal Code makes clear that "no criminal action shall be instituted against a person who commits a crime in a foreign country except by the public prosecutor..." However, the Penal Code does not specify in which cases the public prosecutor can derogate from the general rule and assert extra-territorial jurisdiction. Yet it is clear that this is currently the case when any of the offences in Federal Law No. 5 of 2012 have been committed against "the federal government or any of the local governments of the Emirates of the State or any authority or public institution owned by any of them", as made clear by Article 47.

Moreover, Federal Law No. 39 of 2006 dealing with international judicial cooperation on criminal matters provides for extra-territorial jurisdiction. Whilst this law does not expressly include IT crimes, its scope appears wide enough to cover cybercrimes offences for which the sentence is at least one year, as made clear by Article 7.

However, Interviewee C pointed out that the assertion of extraterritorial jurisdiction was hindered by the lack of specific procedural rules. This makes it difficult to establish beyond reasonable doubt that a person is guilty, which is a prerequisite to extent jurisdiction abroad pursuant to Article 11 of Federal Law No. 39 of 2006. Article 11 of Federal Law No. 39 of 2006 makes clear that a diplomatic channel has to be used for requests to surrender criminals and extradition of criminals is therefore not automatic. As explained by Interviewee D:

> *"If the criminal is out of the United Arab Emirates and committed a crime and such crime caused damage to any person or company or any other entity within the country and such impact extends to the United Arab Emirates, we enter into a diplomatic coordination procedures and seek legal authorisation from the competent authorities in the country where the criminal act occurred. However, there are countries that are developed and advanced with which coordination is possible...but generally there are difficulties in international coordination and cooperation by other countries."*

It was pointed out that this problem can only be overcome through the conclusion of international and bilateral agreements which obligate member countries to enhance judicial cooperation, including by extraditing offenders. These agreements should be binding on the country and spell out clear and unified procedures. Yet some interviewees doubted that these agreements would always ensure that countries provide

judicial assistance to other countries which wish to obtain evidence or seek to extradite criminals. It was explained that one such agreement is the Riyadh Arab Convention on Judicial Co-operation. Article 38 of the Riyadh Arab Convention on Judicial Co-operation makes clear that "persons found…charged with having committed a crime by the competent authority or convicted of having done so by a judicial body of any other contracting parties" can be extradited to other contracting parties. Yet at present use of this Convention is hindered by the contracting parties not having agreed "a joint interpretation of the provisions of the Convention in order to enhance its application."[1255]

Nonetheless, the conclusion of binding mutual legal assistance treaties was deemed another important strategy. The UK has also entered into various international mutual legal assistance agreements, such as the Convention on Mutual Assistance in Criminal Matters between Member States of the European Union 2000 and its Protocol, as well as bilateral mutual legal assistance treaties with various countries.[1256] Similarly, the UAE has entered into bilateral mutual legal assistance treaties, for instance, with India in 1999,[1257] in 2006 with the UK in 2006,[1258] with Australia in 2007,[1259] with Indonesia in

[1255] K. Balz, A. S. Almousa, The Recognition and Enforcement of Foreign Judgements and Arbitral Awards under the Riyadh Convention 1983, Third Years of Arab Judicial Co-operation, 4(2) *International Journal of Procedural Law* 2014, 273-288, 273
[1256] C. Nicholls, C. Montgomery, J. B. Knowles, A. Doobay, M. Summers, *Nicholls, Montgomery, and Knowles on The Law of Extradition and Mutual* (3rd ed, Oxford, Oxford University Press 2013) 314
[1257] Dubai Courts, 2017 <http://www.dubaicourts.gov.ae/portal/page/portal/dc/Legislation_Details?_piref292_457219_292_455214_455214.called_from=1&_piref292_457219_292_455214_455214.law_key=611> accessed 28th February 2017
[1258] C. Nicholls, C. Montgomery, J. B. Knowles, A. Doobay, M. Summers, *Nicholls, Montgomery, and Knowles on The Law of Extradition and Mutual* (3rd ed, Oxford, Oxford University Press 2013) 314
[1259] WAM, UAE, Australia sign two extradition and legal assistance treaties, 30 July 2007 <http://wam.ae/en/details/1395227894411> accessed 28th February 2007

2014[1260] and with Italy in 2015.[1261] The UAE should thus increase its efforts to further enter into bilateral mutual legal assistance treaties. In addition to entering into bilateral and multilateral treaties, the UAE should afford reciprocal treatment to other countries through its cybercrime legislation, especially when no treaties have been concluded with a particular country. [1262] This will help realise joint gains in the fight against cybercrime.[1263] Alternatively, it could include a provision which makes clear that cyber criminals will be punished who have perpetrated cybercrimes in any other country, so long as the offence is also one in the UAE i.e. it could adopt a similar provision as the UK, as discussed above.

It was suggested by the interviewees that at the international level an independent inter-governmental Cybercrime Action Task Force could be set up to promulgate policies to protect the digital realm against cyber criminals, similar to the Financial Action Task Force (FATF). Hence, it was advocated that worldwide recommendations are issued, so that coordination is improved, criminals can be extradited, funds can be recovered, and the same procedures are followed when investigations and searches are conducted and information is exchanged. It was observed that these standards ought to also apply to companies, such as internet service providers, so that fast and uncomplicated procedures are in place to facilitate coordination and cooperation. This was considered to make

[1260] Indonesian Embassy, Indonesia and UAE signed Agreement and Extradition and Mutual Legal Assistance, 3 February 2014 <http://indonesianembassy.ae/indonesia-uae-signed-extradition-agreement-and-mutual-legal-assistance/> accessed 28th February 2017

[1261] UAE Interact, UAE and Italy sign two agreements on judicial cooperation, 18 September 2015 <http://www.uaeinteract.com/docs/UAE_and_Italy_sign_two_agreements_on_judicial_cooperation/71128.htm> accessed 28th February 2017

[1262] M. E. Smith, *Europe's Foreign and Security Policy: The Institutionalization of Cooperation* (Cambridge, Cambridge University Press 2004) 17

[1263] Ibid

cybercrime detection easier and was thought to deter cyber criminals, thereby leading to a reduction in cybercrime rates.

Cooperation with other countries was therefore considered paramount. However, one of the interviewees observed that cooperation amongst GCC countries was not as advanced as in Europe where the Convention on Cybercrime of the Council of Europe (the Budapest Convention) applies. This is despite the adoption of the Arab Convention on Combating Information Technology Offences 2010 (Arab Convention), which includes provisions to promote cooperation between the Arab States. Similar to the Budapest Convention, which requires countries to adopt reciprocal laws and investigate these in their respective territories,[1264] Article 5 of the Arab Convention mandates that state parties criminalise the acts spelled out in the Convention in Articles 6-21. Like the Budapest Convention[1265], the Arab Convention spells out in respect of which cybercrime offences state parties can ask that a person is extradited, namely those listed in Articles 6 to 19 and any other offences committed by means of information technology.[1266] The Arab Convention also contains provisions which require state parties to provide mutual assistance, including through information sharing, so that cybercrime investigations are facilitated.[1267] Practically, this means that internet service providers have to provide

[1264] Also see Article 23 of the Council of Europe Cybercrime Convention; J. B. Hill, N. E. Marion, *Introduction to Cybercrime: Computer Crimes, Laws, and Policing in the 21st Century* (Santa Barbara, ABC-CLIO LLC 2016) 236
[1265] Also see Article 24 of the Council of Europe Cybercrime Convention
[1266] Articles 22(2)(a)-(b) and Article 31 of the Arab Convention on Combating Information Technology Offences 2010
[1267] Also see Articles 25-26 of the Arab Convention on Combating Information Technology Offences 2010; also see Articles 25-26 of the Council of Europe Cybercrime Convention

information when this is required.[1268] Its provisions are very similar to the Budapest Convention, except that it does not require state parties to assist countries with which no treaty has been entered into.[1269] Article 22(1) of the Arab Convention also obligates state parties to "commit itself to adopting, in its domestic law, the legislations and *procedures* necessary to specify the powers and procedures set forth in Chapter III of this Convention."

However, as explained by all the interviewees the UAE lacks a procedural law/code and technical measures. For instance, it was noted that cybercrimes have a procedural aspect, but that it is not explained how cybercrime should be dealt with, e.g. how electronic investigation should be conducted, how evidence should be collected, examined and retained. This was considered problematic, especially in light of the fact that there exist procedural and practical difficulties when conducting digital investigations, evidencing cybercrime and identifying offenders. In this context, Interviewee C remarked:

> *"The procedural difficulties are related to following up/tracking evidence and coordinating with the competent authorities when detecting cybercrimes, especially if the evidence is out of the country. It is also difficult to identify the actor/doer/ offender especially if he/she is out of the country and to freeze seized funds if such funds are out of the country. Additionally, social media, applications and software companies, such*

[1268] J. B. Hill, N. E. Marion, *Introduction to Cybercrime: Computer Crimes, Laws, and Policing in the 21st Century* (Santa Barbara, ABC-CLIO LLC 2016) 237
[1269] Also see Articles 27-28 of the Council of Europe Cybercrime Convention

> *Instagram, Twitter, WhatApp and Facebook, often refuse to cooperate even with officials from their own country, whether at the stage of data collection or at trial. They refuse to provide user data under the excuse of protection of privacy."*

Also, evidence can be easily copied and without rules in place which stipulate how digital evidence ought to be handled, evidence may be doubted. Criminals may thus escape their punishment. The majority of interviewees stressed that the procedural rules in the Federal Law No. 35 of 1992 concerning the Criminal Procedural Law are too general and cannot be transposed to the digital world. They are therefore inadequate for cybercrimes, as Interviewee C asserted:

> *"Special procedures are required, as the patterns of cybercrime are different from traditional crime. For example, the inspection permit for IT crimes are of a special nature to which we cannot apply the traditional criminal code as retention of evidence during the inspection of the device is different."*

The failure by the UAE to adopt procedural laws, codes or guidance also makes it not possible to transpose the following obligations in the Arab Convention, namely to adopt procedures to ensure the expeditious custody of data stored in information technology (Article 23) and the expeditious custody and partial disclosure of users tracking information (Article 24). The UAE also lacks "procedures to enable the competent

authorities to issue orders to...submit certain information...stored on information technology...[or from] any service provider..." (Article 25), "procedures ...to enable its competent authorities to inspect or access" stored information (Article 26); "procedures...to enable the competent authorities to seize and safeguard" stored information (Article 27); procedures to gather users tracking information (Article 28); and legislative procedures to enable the authorities to intercept content information (Article 29). In contrast, in the UK the NPCC has published the Good Practice Guide for Digital Evidence 2011, the Good Practice Guide for Computer-Based Electronic Evidence and the Good Practice Guide for Managers of e-Crime investigation.[1270] Hence, the procedures are clearly spelled out which have to be followed when e-crime is being investigated and electronic evidence is being handled, in contrast to the UAE where this has not yet been done.

According to the interviewees, the main shortcoming with UAE's e-crime legislation is therefore that no procedures have been enacted and this makes it difficult to enforce cybercrime offences. Similarly, Kshetri observes that enacting cybercrime laws is straightforward, but that the challenge is to create enforcement mechanisms.[1271] There was overwhelming agreement that procedural rules should be developed and that a law should be adopted which informs how electronic evidence should be dealt with.

[1270] The Association of Chief Police Officers Good Practice Guide for Digital Evidence 2012, <http://www.acpo.police.uk/documents/crime/2011/201110-cba-digital-evidence-v5.pdf> accessed 2 May 2014; the Association of Chief Police Officers Good Practice Guide for Computer-Based Electronic Evidence, <http://www.7safe.com/electronic_evidence/ACPO_guidelines_computer_evidence.pdf> 2 May 2014; the Association of Chief Police Officers Good Practice Guide for Managers of e-Crime Investigation, <http://www.acpo.police.uk/documents/crime/2011/201103CRIECI14.pdf> accessed 2 May 2014

[1271] N. Kshetri, *The Global Cybercrime Industry: Economic, Institutional and Strategic Perspectives* (London, Springer 2010) 148

Procedures should be spelled out and it should be made clear that a failure to follow these procedures results in the prosecution not being permitted to rely on the evidence. It was mentioned that Qatar had enacted a cybercrime law, which addressed procedural aspects. It was strongly recommended that a permanent cybercrime committee is formed which is composed of members from the police, prosecution, the judiciary, the communication authorities, corporations and security agencies. Such permanent committee would be authorised to review laws and would consider whether provisions have to be amended. Importantly, such a committee ought to be entrusted with promulgating procedural rules. These rules would not necessarily have to be in form of law, but instead this could be in the form guidance, as in the UK. Yet as also made clear by Article 29 of the Arab Convention on Combating Information Technology Offences 2010, additionally *legislative procedures* have to be adopted to enable the authorities to intercept content information. Consequently, it is also important for the UAE to enact surveillance and data retention laws.

5.1.3 Surveillance and Data Retention Laws

Cybercrime can arguably only be successfully combated through technology-driven strategies. Law enforcement agencies must therefore be granted "new powers of search and seizure" in order to investigate crime.[1272] As many aspects of daily life now take place online, this means requiring internet service providers (ISPs) to offer intercept technology, so that enforcement agents can legally access data transmissions and are assisted when searching data traffic and can request information about customers and

[1272] L. Huey, R. S. Rosenberg, Watching the Web: Thoughts on Expanding Police Surveillance Opportunities under the Cyber-Crime Convention, *Canadian Journal of Criminology and Criminal Justice* 2004, 597-606

access retained data.[1273] This effectively means "convert[ing ISPs] into integral cogs in the apparatus of online law enforcement" and "establishing 'policing' networks with elements of the private sector...that have the tools and capacity to achieve desired results beyond the state..."[1274] Certainly, this implies a trade-off with the rights of normal internet users.[1275] However, as observed by the interviewees surveillance takes place already to a certain extent in all countries. For instance, there are cameras on the streets in most cities around the world in order to monitor people. Whilst some may perceive this to be an interference with their personal freedom, this was considered a necessary precaution to protect the public against crime. Similarly, mass surveillance means that the same logic is applied to the virtual world. Information Communication Technologies (ITCs) are employed to control crime and to reap policing efficiency.[1276] The interviewees therefore considered interception of communications necessary to protect against the dangers which technology poses to the UAE. In this context, Interviewee D commented:

> *"Granting surveillance powers will facilitate detection of crimes… The existence of complicated procedures and long correspondences to obtain permission leads to a loss of evidence and helps criminals to escape, especially cyber criminals. Granting such powers will have a big effect on detecting criminals and will limit cybercrime, as evidence can be obtained quickly."*

[1273] Ibid
[1274] Ibid
[1275] M. N. Sirohi, *Transformational Dimensions of Cybercrime* (Delhi, Alpha Editions 2015) 52
[1276] M. S. Nuth, Taking advantage of new technologies: For and against crime, 28 *Computer Law & Security Report* 2008, 437-446, 437

The need for surveillance powers is also underscored by the fact that at present there is a large number of cases registered against unknown persons in the UAE. This is because the authorities are often unable to access data and to identify offenders, especially when crimes are committed in other countries. Also, as discussed above, both the Arab Convention on Combating Information Technology Offences 2010 and the Convention on Cybercrime of the Council of Europe mandate electronic monitoring and data surveillance, which is important as part of a pro-active policing approach.[1277] Already in 2000, the UK passed the Regulation of Investigatory Powers Act 2000 and the Terrorism Act 2000 which confer broad powers on government bodies to conduct surveillance [1278], as discussed in Chapters 1 and 3. Additionally, it enacted the Investigatory Powers Act 2016 which further legalises various tools for hacking and snooping by enforcement agents.[1279] In contrast, the UAE has to this present date not enacted a legislative framework for surveillance and data retention. This was identified as a serious problem by all the interviewees.

This is not to say that no surveillance takes place. Interviewee E stated:

> *"The police contact the service providers and request it to provide information after a court orders this. I do not know of a system which*

[1277] N. Abouzakhar, *ECCWS 2015 14th European Conference on Cyber Warfare and Security, Hatfield UK* (Reading, Academic Conferences and Publishing International Ltd 2015) 302
[1278] P. Mobbs, Privacy and Surveillance, How and when organisations and the state can monitor your actions, GreenNet Civil Society Internet Rights Project, 2003, 1-11, 5 <http://www.internetrights.org.uk/briefings/irtb05-rev1-draft.pdf> accessed 29 June 2014
[1279] E. Macaskill, 'Extreme surveillance' becomes UK law with barely a whimper, 19 November 2016 <https://www.theguardian.com/world/2016/nov/19/extreme-surveillance-becomes-uk-law-with-barely-a-whimper> accessed 28th February 2017

specifies the method of requesting information other than by a court order and everything is done through a specific court order."

Moreover, it was explained that the telecommunications services provider Etisalat and the Telecommunications Regulatory Authority have large powers to conduct surveillance and to intercept data. Specialised staff and competent authorities can intercept all data in the country in order to investigate crime. Also, at most police stations, there is a section which deals with IT crime. Officers, who work for this section, have powers to conduct digital investigations and to collect electronic evidence. Additionally, the Minister can authorise more comprehensive and invasive powers to collect information, e.g. the police or the Telecommunications Regulatory Authority. Yet several of the interviewees observed that these powers had only been granted through internal regulations.

However, it was noted that surveillance only takes place after an authenticated source reports that a crime has been committed. The same reactive approach can be found in Article 43 of Federal Law No. 5 of 2012, which states that "the court may order to put the condemned under surveillance..." This is different to the pro-active UK approach, which is much more sweeping, as discussed in Chapter one and three. For instance, the UK's Government Communications Headquarters (GCHQ) ran the Tempora programme under which all individuals were subjected to bulk surveillance, irrespective of whether

or not they were under a suspicion of having committed a crime or not.[1280] Yet the interviewees were divided about whether interception of communications and bulk collection of communications data are impermissible, as some felt that this should only be specified in the inspection permit. Accordingly, only specific data should be obtained. All of the interviewees cautioned that surveillance requires legal authorisation. Some argued that granting enforcement personnel too expansive surveillance powers is unwise, also since it conflicts with protecting the privacy of individuals. For instance, Interviewee C asserted:

> *"Allowing surveillance under the pretext of preventing cybercrimes should not be allowed since this results in privacy infringement. However, conditional surveillance is warranted in respect of some crimes, e.g. terrorism and serious criminal cases and cases where state security is being prejudiced."*

It was explained that conditional surveillance should mean that a judicial body authorises the surveillance and the specific powers on each occasion. In contrast, another interviewee opined that the police require more comprehensive and invasive powers to collect information, so long as this is within the limits of not infringing the privacy of persons and in a manner which accords with the stipulated procedures. All the interviewees agreed that a balance has to be struck between surveillance powers and protecting the privacy of individuals. Similarly, the European Court of Human Rights

[1280] O. Bowcott, UK-US surveillance regime was unlawful 'for seven years', The Guardian, 6 February 2015 <https://www.theguardian.com/uk-news/2015/feb/06/gchq-mass-internet-surveillance-unlawful-court-nsa> accessed 28th February 2017

has made clear that the power to conduct surveillance is not unlimited, but that the *"interest of a state in protecting its national security must be balanced against the seriousness of the interference with the applicant's right to respect for his or her private life."*[1281]

Article 31 of the UAE constitution states that "freedom of communication by post, telegraph or other means of communication and the secrecy thereof shall be guaranteed in accordance with the law." However, without a law which defines the parameters of this freedom and guarantee, surveillance is arguably illegitimate, as pointed out by one interviewee. He therefore emphasised that a surveillance law should be enacted, so that the powers of enforcement agents are explained, as well as the limits when investigating crimes. Several of the interviewees noted that surveillance is presently subject to Federal Law No. 35 of 1992 concerning the Criminal Procedural Law. Yet all of the interviewees thought that this law was inadequate and that this constituted a problem.

The interviewees therefore recommended that surveillance powers are put on a statutory footing, so that basic constitutional rights are not prejudiced and the circumstances and procedures are clearly spelled out. Without this it was felt that there was a legislative gap which made combating cybercrime more challenging. The interviewees explained that such a surveillance law should detail which information can be acquired and in case other information is collected, this should be rendered unlawful. In such a case, the information should not be relied upon.

[1281] *Rotaru v Romania* (2000) 8 BHRC 449

In the context of surveillance, it was emphasised that data retention is also necessary. Interviewee B explicated that data retention was of "*great importance in the detection of crime."* The police and other agencies may need data later in order to identify offenders. Other interviewees also stressed that data retention was extremely necessary. Whilst in Europe data retention was in response to the terrorist attacks in Madrid and London[1282] and there have been no terrorist attacks in the UAE to date, they are nonetheless *"likely",* as *"[t]errorists continue to issue statements threatening to carry out attacks in the Gulf region."*[1283] Accordingly, the UAE should consider permitting data retention to protect *"national security, defence, public security or the prevention, investigation, detection, and prosecution of criminal offences of unauthorised use of the electronic communications system."*[1284]

However, as explained by Interviewee C, *"We have no legal powers to retain data."* Instead this is currently done through internal regulations adopted by the Telecommunications Regulatory Authority. It was unclear whether the timeframe for keeping data and the type of data are detailed in these regulations. Hence, a rather informal approach has been adopted. This is problematic, as highlighted by the recent findings by the UK Investigatory Powers Tribunal which ruled that the secretly run Tempora programme by GCHQ was illegal.[1285] Nonetheless, the Investigatory Powers

[1282] T. Konstadinides, Destroying democracy on the ground of defending it? The Data Retention Directive, the surveillance state and our constitutional ecosystem, 36(5) *European Law Review* 2011, 722-736, 724
[1283] UK Government, Foreign travel advice, United Arab Emirates, Terrorism, 2017 <https://www.gov.uk/foreign-travel-advice/united-arab-emirates/terrorism> accessed 28th February 2017
[1284] Article 15 of the now defunct European Union Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector; C. Walker, *Terrorism and the Law* (Oxford, Oxford University Press 2011) 75
[1285] O. Bowcott, GHC surveillance hearing to begin, The Guardian, 14 July 2014 <https://www.theguardian.com/uk-news/2014/jul/14/court-gchq-surveillance-tempora-ipt-nsa-snowden>

Tribunal held that principally the RIPA permits mass surveillance in respect of all fibre optic cables which leave or enter the UK.[1286] This is because data which has been acquired through *"bulk interception cannot be used to search for and examine the communications of an individual in the UK unless GCHQ first obtain a specific authorization naming that individual, signed by a secretary of state."*[1287]

All interviewees concurred that it would be better if a law was enacted which required telecommunication providers and ISPs to retain data and which specifies the controls when data is retained. It was thought that the data should remain with the service provider Etisalat. The punishment should be specified i.e. whether criminal or administrative sanctions should be imposed in case Etisalat wrongly deletes data. Such a law should also address whether joint or several liability should be imposed on Etisalat or staff in cases where Etisalat is required to retain data, but staff unintentionally delete data. The sanctions for unlawfully accessing retained data without special authorisation must also be detailed. It was pointed out that Federal Law No. 5 of 2012 can be evoked in cases where staff illegally access, publish or circulate data. The service provider can also be punished by virtue of the Federal Law by Decree No. 3 of 2003 on Telecom Law and staff can be pursued for data infringement. Accordingly, abuse of broad enforcement powers results in staff exposing themselves to criminal liability. Other provisions also regulate privacy infringements by staff and other types of abuse of

---

accessed 1st March 2017; O. Bowcott, UK-US surveillance regime was unlawful 'for seven years', The Guardian, 6 February 2015 <https://www.theguardian.com/uk-news/2015/feb/06/gchq-mass-internet-surveillance-unlawful-court-nsa> accessed 28th February 2017

[1286] Privacy International, Investigatory Powers Tribunal rules GCHQ mass surveillance programme TEMPORA is legal in principle, 18 December 2014 <https://www.privacyinternational.org/node/46> accessed 1st March 2017

[1287] M. O. Jalaalzaai, *Fixing the EU Intelligence Crisis: Intelligence Sharing, Law Enforcement and the Threat of Chemical, Biological, and Nuclear Terrorism* (New York, Algora Publishing 2016) 96

powers. Yet it should be reviewed whether the sanctions in Federal Law No. 5 of 2012 and Federal Law by Decree No. 3 of 2003 on Telecom Law are appropriate in cases where enforcement agents access data. It may be important to devise certain exceptions, for instance, in urgent cases where cyber attacks pose the risk of loss of life, serious damage to national security, serious injury or illness.

As discussed in Chapter 3, the UK RIPA spells out powers when communications are intercepted.[1288] Additionally, it explains the procedures when intrusive surveillance can be conducted,[1289] as well as which requirements have to be met to use Covert Human Intelligence Sources.[1290] It also discusses the powers in respect of directed surveillance.[1291] Similarly, the UAE should spell out different procedures for the different types of surveillance powers, it may want to equip law enforcement agents with. In this context, it should also grant fewer bodies the right to conduct more intrusive surveillance, e.g. directed surveillance.[1292]

In terms of the type of data, which should be retained, Interviewee B thought that this should particularly consist of data which identifies a person's identity, as well as the activities which he performed whilst accessing the internet. Another interviewee thought that different types of data ought to be retained, i.e. medical authorities should retain health data, Etisalat should retain personal data about their customers, including calls

[1288] See Part 1 of the RIPA, especially s.24(5)(2)
[1289] See Part 2 of the RIPA
[1290] See Part 2 of the RIPA
[1291] See Part 2 of the RIPA
[1292] S.24(5)(4) of RIPA; J. Alder, *Constitutional and Administrative Law* (10th ed, London, Palgrave 2015) 569

and messages, employers should keep data about their employees, etc. Mobile phone data was particularly deemed important, including the address of the person who owns the phone, as well which other persons s/he has contacted, whether in the UAE or abroad. It was suggested that the remaining data could be retained by specialised technicians. However, Interviewee D expressed a difference of opinion:

> *"It is difficult to separate data and in my opinion interception should be comprehensive as one may find something which indicates that a person has committed a crime. Interception should be limited to whatever proves the commission of the crime by the person or which helps detecting the crime. The police should be trusted when they deal with persons' data and should therefore not use such data beyond the limits of the case which they are investigating and such data should be kept top confidential."*

This view largely accords with the approach taken under UK law, where for instance, a minister has to issue a warrant in order to intercept communication data[1293] and where such material has to be destroyed when there are no longer *"authorised purposes"* or an offence is committed.[1294]

However, additionally it was emphasised that the content of websites should be monitored, as some propagate terrorist ideas or advertise fake jobs designed to lure people into the country and these should be blocked.

[1293] S. Foster, *The Judiciary, Civil Liberties and Human Rights* (Edinburgh, Edinburgh University Press 2006) 141

[1294] S.15(4) and s.19 of RIPA; B. Emmerson, A. Ashworth, A. Macdonald, *Human Rights and Criminal Justice* (3rd ed, London, Sweet & Maxwell 2012) 328

It was suggested that regulations could be issued by the Telecommunications Regulatory Authority for Etisalat and Emirates Integrated Telecommunications Company (Du) in order to assist law enforcement agents with surveillance. These could set out controls and the compliance departments of these firms could be required to verify compliance. Controls for staff access would have to be detailed and whilst they would not have to be absolute, this could consist of staff, who access a piece of information, being required to state the reason for this. It was recommended that the extent of access should be commensurate with the investigatory needs of the law enforcement agent.

Furthermore, Interviewee D stressed that investigatory authorities ought to cooperate and coordinate with Etisalat and Du, as well with social network providers, so that their networks can be intercepted when data is required for investigations.

It was discussed that any new law ought to set out the timeframe for the data retention. One interviewee stated that the duration should depend on the type of data i.e. if it is important data it should be retained, even if it does not relate to a crime. Accordingly, data which may be needed to detect crimes later on should be kept for longer periods. It was thought that retention of basic data may burden the service provider and should only be retained for a shorter period, e.g. for six months, whereas important data should be kept for three years. In contrast, Interviewee B thought that data should be retained between six months and up to one year, whereas Interviewee C thought that the maximum period should be three months. It was also suggested that laws in other

countries should be studied when setting the timeframe and that the costs for retaining the data should be taken into account. Interviewee D pointed out that a longer data retention period was obviously better, but that it should fall on the Telecommunications Regulatory Authority to determine the period. For instance, the Telecommunications Regulatory Authority could issue a retention notice which requires Etisalat and Du to retain data and this notice could specify the retention period, as well as any other conditions. Hence, a similar set up could be adopted as in the UK, where the Secretary of State is in charge of this.[1295]

All the interviewees agreed that it is important to adopt legal powers which detail the procedures for decryption requests. It was explained that just like with traditional crimes, where the police may have to break a door in order to get access to a crime location or to catch an offender, the same applies to the digital realm. Otherwise, fences may be created to detect crime. Specialists must therefore decrypt data, especially when serious investigations are pursued or to obtain evidence which proves that a crime has been committed. It was pointed out that this was not a task for the police in general, but a matter for the electronic evidence laboratory.

The interviewees made clear that at present there exists no power to request companies to provide data from customers in order to decrypt it. It was thought that such a power would be difficult to reconcile with the right to privacy. It was suggested that decryption requests should require an authorisation from the courts. Also, the Commander-in-chief of the police could issue a warrant or sign one subsequently, similar to the UK where

[1295] S.1 of the UK Data Retention and Investigatory Powers Act 2014

this power lies with the Secretary of State, judges and the Surveillance Commissioner.[1296]

Interviewee C suggested that in cases where the authorities fail to decrypt a digital device, the accused ought to be requested to prove his/her innocence i.e. that the device contains no evidence which incriminates him/her. The accused would thus have to prove that he/she did not commit the crime and has nothing to hide on his/her digital device and is ready to provide access. A refusal by the accused would not constitute evidence that s/he has committed the crime, but together with any other evidence, would support the case against the accused.. The vital importance of the presumption of innocence was highlighted in *Woolmington v DPP*[1297] where the 'golden thread', as it is called, was established by Viscount Sankey making it clear in unambiguous terms that the onus of proof should lie on the prosecution. Despite the 'golden thread' it would be 'misleading to imagine that reverse burden provisions are in some way anomalous in criminal law.'[1298] Even though such a reversal of the onus does raise some questions with respect to Article 6 of the European Convention on Human Rights, the European Court of Human Rights in *Salabiaku v France*[1299] clarified that not all provisions that impose the legal burden on the accused will infringe Art.6(2) and that such provisions are not

[1296] S.24(5)(4) of RIPA; J. Alder, *Constitutional and Administrative Law* (10th ed, London, Palgrave 2015) 569
[1297] *Woolmington v DPP* [1935] AC 462.
[1298] Ben Fitzpatrick, 'Reverse burden and Article 6(2) of the European Convention on Human Rights: official secrets' (2008) 72(3) JCL 190, 193.
[1299] *Salabiaku v France* (1988) 13 EHHR 379.

prohibited, however they should be confined within reasonable limits, In the case of *R v Lambert*[1300] Lord Hope held that:

'*It is now well settled that the principle which is to be applied requires a balance to be struck between the general interest of the community and the protection of the fundamental rights of the individual. This will not be achieved if the reverse onus provision goes beyond what is necessary to accomplish the objective of the statute'*[1301]

The Court in *Lambert* specified that in order for such a reversal to be accepted it will need to be just and proportionate for the aim it seeks to achieve Also, having in mind the nature of the situation in question it is likely to be considered not only proportionate but also reasonable for the onus to be reversed, as it would indeed be more easy and practical for innocence to be proved, instead of the opposite[1302]

Hence, a reverse onus could operate, in such situations subject to what has been discussed above, yet this alone may not be sufficient to effectively combat cybercrime. It would be better if additionally, enforcement officers had the power to request those who may reasonably have the key to decrypt legally seized devices, so long as a warrant has been issued to that effect or a judge has permitted this.[1303] This approach has been adopted by the UK and makes it possible for devices to be decrypted through cooperation, e.g. with manufacturers. In the UK, these decryption requests are often

[1300] *R v Lambert* [2002] AC 545.

[1301] *R v Lambert* [2002] AC 545 (Lord Hope).
[1302] *Gatland v Commisioner of Police of the Metropolis* [1968] 2 WLR 1263.
[1303] S.49(2) of RIPA; Schedule 2, Articles 1(1)(a) and 2 of RIPA

accompanied by secrecy undertakings, so that those which have been requested cannot disclose that this has been done to the person.[1304]

All the interviewees made clear that it was not a good strategy to weaken or ban encryption.

On the subject Interviewee E said:

> *"I think* [*Encryption*] *is important for communication companies and for various bodies that possess data such as banks and companies. Data should be encrypted for the purpose of secrecy and data protection because the absence of encryption may lead to very easy access to information by criminals, in addition to that, the users will not feel their information is securely retained and through a secured network…"*

Also, in the UK there exists no ban on end-to-end encryption, though this was initially proposed.[1305] Instead companies can be ordered to decrypt devices in practicable cases by virtue of the Investigatory Powers Act 2016.[1306] It was discussed that there has been an interest in creating backdoors for law enforcement officers to access encrypted content, including commercial data, when a crime has occurred. Yet it was thought that a court should grant such a power in specific cases and that specific procedures should

[1304] B. J. Goold, D. Neyland, *New Directions in Surveillance and Privacy* (Cullompton, Willan Publishing 2009) 50

[1305] K. Collins, UK surveillance law marks a 'worse than scary' shift, CNET, 29 November 2016 <https://www.cnet.com/uk/news/snoopers-charter-investigatory-powers-bill-royal-assent-surveillance-uk/> accessed 1st March 2017; A. J. Martin, UK gov says new Home Sec will have powers to ban end-to-end encryption, The Register, 14 July 2016 <https://www.theregister.co.uk/2016/07/14/gov_says_new_home_sec_iwilli_have_powers_to_ban_endtoend_encryption/> accessed 1st March 2016

[1306] Ibid (Collins)

be in place to regulate this. In the UK, security and law enforcements agents can hack particular phones, devices or computers i.e. can engage in "equipment interference and can also bulk hack foreign targets when this is authorised.[1307] For this purpose, an Equipment Interference Draft Code of Practice has been issued by the Home Office.[1308] Any future legislation should therefore spell out in which cases law enforcement agents have the power to make decryption requests, as well as the procedure. The same would have to be done for equipment interferences, so that the power is clearly spelled out, as well as the procedures and ideally a code of guidance should be issued.

5.1.4 Privacy and Data Protection

As discussed above, the failure to define the concept of privacy infringement and personal data has resulted in cyber criminals escaping their just punishment. Privacy infringement was considered a crime by the interviewees, as is also made clear in Article 21 of Federal Law No. 5 of 2012, which criminalises using a *"computer network... or any information technology means for the invasion of privacy..."* Yet a balance has to be struck between "*freedom from unauthorized intrusion"* [1309] and security. It was thought that this can only be achieved through clear legal provisions which detail the powers of law enforcement bodies. Surveillance, interception, data retention, decryption and other law enforcement powers were deemed necessary in order

[1307] J. Vincent, The UK Now Wields Unprecedented Surveillance Powers - Here's What It Means, The Verge, 29 November 2016 <http://www.theverge.com/2016/11/23/13718768/uk-surveillance-laws-explained-investigatory-powers-bill> accessed 1st March 2017

[1308] Home Office, Equipment Interference, Draft Code of Practice, Autumn 2016, 1-97 <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/557861/IP_Bill_-_Draft_EI_code_of_practice.pdf> accessed 1st March 2017

[1309] Merriam Dictionary <http://www.merriam-webster.com/dictionary/privacy> accessed 20th January 2015; H. Sarfaraz, Surveillance, privacy and cyber law, 20(7) *Computer and Telecommunications Law Review* 2014, 189-194, 189

to investigate whether or not a crime had been committed. In this context, interviewee A stated:

> *"Preventative policing ought not prejudice the privacy of individuals. Only if information suggests that a person is involved in a crime should his data be accessed after the competent authorities have authorised this."*

However, in light of the fact that predictive policing is *"the future of law enforcement"*, policing has to become *"less reactive."*[1310] Predictive policing means that different types of information are gathered and technology is employed to obtain intelligence, so that crime can be fought.[1311] As observed by Professor Elizabeth Joh *"soon it will be feasible and affordable for the government to record, store and analyse nearly everything we do*" and the police will get alerts through computer programs which analyse huge data sets in order to identify suspicious activities.[1312] Cybercrime has arguably led to this new policing model since it has called into doubt the effectiveness of the traditional reactive policing paradigm.[1313] The standard law enforcement model is based on deterrence, successful crime investigation and controllable injury caused by disorder, as also discussed in Chapter 1.[1314] Yet in the digital world, criminals can be anonymous, cannot be traced, employ encryption and the crime can be distributed,

---

[1310] B. Pearsall, Predictive Policing: The Future of Law Enforcement? 266 *National Institute of Justice Journal* 2010, 16-19, 16-17
[1311] J. W. Osterburg, R. H. Ward, *Criminal Investigation: A Method for Reconstructing the Past* (7th ed, Abingdon, Routledge 2014) 266
[1312] J. Sadowski, Police data could be labelling 'suspects' for crimes they have not committed, The Guardian, 4 February 2016 <https://www.theguardian.com/technology/2016/feb/04/us-police-data-analytics-smart-cities-crime-likelihood-fresno-chicago-heat-list> accessed 1st March 2017
[1313] N. Kozlovski, A Paradigm Shift in Online Policing - Designing Accountable Policing, Yale Law School, 2005, 1-22, 7 <https://crypto.stanford.edu/portia/papers/Kozlovski.pdf> accessed 1st March 2017
[1314] Ibid, 8

automated and international.[1315] A preventative and thus proactive policing model is technologically and economically more effective.[1316] However, this requires that the tension between predictive policing facilitated through surveillance and data collection and analysis of such data is bridged, for instance, through *"a thorough privacy policy, training personnel to use it properly, enforcing accountability and continually refining the policy."*[1317] Trustworthy processes have to be adopted which are transparent and can be audited.[1318] This requires that procedures are enacted, which all interviewees identified as one of the main shortcomings within the current e-crime framework of the UAE.

The great majority of interviewees therefore emphasised that it was important for the UAE to improve its data protection laws, both procedurally, for instance, through the adoption of a "*thorough privacy policy"*[1319] by law enforcement agents and in terms of the available sanctions. For instance, such a policy could include a collection limitation principle (i.e. personal data should only be collected through fair and legal means and where possible with the knowledge of the data subject); a purpose specification principle (i.e. the use should be made clear prior to the data collection and further use should be limited accordingly); a use limitation principle (i.e. the use can only be for the specified purpose); a data quality principle (i.e. the data has to be accurate, relevant and up-to

[1315] Ibid
[1316] Ibid
[1317] B. Pearsall, Predictive Policing: The Future of Law Enforcement? 266 *National Institute of Justice Journal* 2010, 16-19, 18
[1318] Ibid
[1319] Ibid

date); and an individual participation principle (i.e. the data subject should be entitled to certain rights, e.g. to find out which data is held about him/her.[1320]

One of the first steps which should be taken is to clarify the concept of privacy, personal data and data protection in order to remedy the current problems with Federal Law No. 5 of 2012, as discussed above. Yet the interviewees considered that this alone is a too narrow approach and favoured more sweeping reforms; Interviewee C said:

"Data collection by companies is not regulated in the UAE."

The data protection legislation for the Dubai International Financial Centre (DIFC) does not apply to the rest of the UAE.[1321] This was identified as a lacuna in an era where companies collect vast amounts of data about individuals and thereby expose them to security risks. The interviewees concurred that data protection and privacy help preserving network and information security. A data protection reform would promote cultural awareness and would reinforce that employees, including enforcement agents, have to deal carefully with data. Companies would take precautions when they handle personal data, which in turn makes it more difficult for cyber criminals to access such data. In this context, the interviewees recommended that companies which handle personal data should notify security or data protection breaches to the authorities, as well as crimes.

[1320] W. L. Perry, B. McInnis, C. C. Price, S. C. Smith, J. S. Hollywood, *Predictive Policing: The Role of Crime Forecasting in Law Enforcement Operations* (New York, RAND Corporation 2013) 50
[1321] S. Paterson, B. Hopps, N. Lovell, United Arab Emirates, Cybersecurity, Herbert Smith Freehills LLP, 17 March 2016, 1-6, 2

The majority of the interviewees urged the legislator to enact a federal law which addresses data and privacy protection, as expressed here by Interviewee E:

> *"A special data protection law has been issued recently in Qatar, which appears perfect since it complies with the best international practices and is modelled closely on the European law which is considered to be one of the best laws for data and privacy protection."*

Hence, steps should be taken to ensure that the UAE does not fall behind other states in the Middle East, especially since this was thought to heighten the risk of cybercrime, e.g. through careless handling of personal data by companies. This is vital in realising "accountable policing" in an age where proactive policing tactics through surveillance and other preventative strategies have increasingly become more commonplace.[1322]

5.1.5 Evidence Rules on the Admissibility of Digital Evidence and Intercept Material in Criminal Proceedings

The interviewees considered that criminals ought not be informed about intercept material in cases where the criminal thereby finds out how evidence is gathered. Otherwise, criminals will be aware of the way in which information is collected and avoid these sources. This would make it more difficult for law enforcement agents to detect crime and would pose a threat to the security of the nation. It was explained that

[1322] N. Kozlovski, A Paradigm Shift in Online Policing - Designing Accountable Policing, Yale Law School, 2005, 1-22, 20-21 <https://crypto.stanford.edu/portia/papers/Kozlovski.pdf> accessed 1st March 2017

the Department of Evidence deals with the detection of electronic data and evidence, which judges take into account. In this context, Interviewee E remarked that:

> *"Evidence is generally accepted by the court. The court may consider it important to protect the source of the evidence or the technical method through which the evidence has been obtained, but that is up to the discretion of the court."*

It was acknowledged that problems had been encountered with the current evidence rules on the admissibility of digital evidence and intercept material in criminal proceedings. This is because judges are afforded a wide discretion by the failure to enact provisions which stipulate the circumstances and process for the prosecution to not disclose evidence. Without this, there is the risk that the impression is created that there exists no "*open justice."*[1323] The right to a fair hearing implies that the accused receives the evidence which is used against him, so that he can defend himself.[1324] When derogations are made from this important principle, these should be clearly stated since this promotes the rule of law.[1325] For instance, in the UK the accused can challenge the decision that public interest immunity has been granted.[1326] The surveillance law i.e. s.17 of the RIPA also states that intercepted communications are not permitted during court proceedings. Moreover, the judge can request that the intercept material is

[1323] J. Alder, *Constitutional and Administrative Law* (10th ed, London, Palgrave 2015) 561
[1324] G. Martin, R. Scott Bray, M. Kumar, *Secrecy, Law and Society* (Abingdon, Routledge 2015) 4
[1325] Ibid
[1326] *Goodridge v Chief Constable of Hampshire Constabulary* (1999) 1 All ER 896; *Air Canada v Secretary of State for Trade (No.2)* (1983) 2 AC 394; s.3 of the Criminal Procedure and Investigations Act 1996; J. Alder, *Constitutional and Administrative Law* (10th ed, London, Palgrave 2015) 562

inspected by him/her and can order the prosecutor to admit a fact in order to uphold justice.[1327]

Similar procedures could be adopted as part of the internal regulations which judges follow. These could apply to the competent circuit for cybercrimes, which had been created at all federal courts in the country by virtue of a resolution of the Ministry of Justice in 2012 in order to strengthen e-capacity. It was explained that prior to this, cybercrimes were dealt with by misdemeanour circuits, alongside other traditional misdemeanours. These procedures could also be taught as part of the qualification programs in technology and electronic evidence, which have been developed for judges.

Additionally, several of the interviewees recommended that judges are furnished with simple technical reports which explain how the crime has been committed. This would assist them when determining whether or not is guilty of the crime. In the alternative, it was suggested that technical teams ought to detect the crime for the court and should then discuss the crime and evidence in order to convince the judge that the evidence incriminates the accused.

5.2 Summary

This chapter analysed the interviews with various senior experts who deal with cybercrime cases in the UAE, namely the police, the office of prosecution, the judiciary, the Telecommunications Regulatory Authority and Interpol. Their particular experiences were presented in light of the literature discussed in previous chapters. Problems were

[1327] Sections 18(7)(b), 18(8) and 18(9) and s.18(10) of RIPA

highlighted with the existing legislative e-crime landscape in the UAE, as well as their improvement suggestions. The cybercrime offences legislation was particularly studied as this is the main framework. The topics of surveillance, data retention and decryption were discussed. It was analysed whether privacy and data protection laws are needed in order to heighten network and information security, as well as in light of the new preventative policing paradigm. The lack of evidence rules on the admissibility of intercept material was also addressed. These topics were understood viewed through the lens of e-crime practitioners in the UAE and which further enriched the insights which have been gained from the study of the literature in Chapter 1 and the doctrinal analysis of the respective legislative frameworks in the UAE and UK. It is against this background that the next chapter will spell out recommendations, which are intended to strengthen the existing legislative e-crime landscape in order to combat cybercrime more effectively in the UAE.

With these findings in mind, the following chapter concentrates on the legal framework the UAE could adopt to strengthen its fight against cybercrime.

Chapter Six: Developing a Legal Framework to Combat E-Crime in the UAE

6. Introduction

Having critically and empirically explored how e-crime regulations can be improved to combat cybercrime in the UAE in Chapter Five, this chapter presents the legal

framework which the UAE could adopt in order to combat e-crime. The recommendations are based on the black-letter law analysis and the comparative findings, as well as the practical suggestions from the interviews. As discussed in Chapter Four, cybercrime is on the increase in the UAE and businesses and individuals have been targeted by cyber-criminals. At present, the policing approach is not sufficiently proactive and cyber-security risks could therefore be combated more effectively. Whilst various steps have already been taken to secure the digital realm, challenges still exist. The legal framework is not yet particularly sophisticated when one compares it with that of the UK. This is because at present, the main approach has simply consisted of criminalising various acts and the response has been reactive. For example, investigations only take place when offences are being reported. In contrast, in the Western word, predictive and intelligence-led policing facilitated through surveillance and data collection and analysis of such big data is being employed to secure the digital realm.[1328] Such an approach is facilitated by the substantive law, which spells out the regime which governs surveillance and data retention, including the checks and balances which are required to prevent abuse of powers. Moreover, UK privacy and data protection rights provide another layer of protection since they compel organisations to pay greater attention to securing personal data. As personal data are the target of cyber-criminals in order to commit fraud, a more robust and comprehensive approach has been adopted. In contrast, in the UAE data protection has only received scant attention and data protection law is not being fully utilised to heighten data security. The legal regime of the UK is therefore very different to that in the UAE, also

[1328] B. Pearsall, Predictive Policing: The Future of Law Enforcement? 266 *National Institute of Justice Journal* 2010, 16-19, 18

because much more guidance and legal rules have been developed which inform about the relevant procedural rules, which apply to criminal cases that have an e-crime element. Much more cooperation also exists within the EU, whereas the regional regime in the Gulf States is still in its infancy. The challenge for the UAE is, therefore, to adopt a more sophisticated legal framework and the following recommendations are intended to assist with this.

6.1 Surveillance: Towards a More Preventative and Intelligence-Led Policing Model

In the context of cybercrime and crime with an e-element, intelligence-led policing is arguably the best approach.[1329] Intelligence-led policing is future-oriented, as risks and issues are analysed and targeted strategies are devised accordingly.[1330] The topic of crime control is therefore addressed differently than under traditional reactive policing approach.[1331] This is because the focus is on "forward looking" tactics[1332] which are more appropriate for cybercrime as these crimes predominantly take place anonymously, without any warning and extremely quickly from any location in the world. [1333] Intelligence is therefore the only means available in the fight against cybercrime.[1334] Monitoring by law enforcement agents and the private sector is therefore

[1329] M. Dawson, D. R. Kisku, P. Gupta, J. K Sing, W. Li, *Developing Next-Generation Countermeasures for Homeland Security Threat Prevention* (New York, IGI Global 2016) 87
[1330] M. Maguire, T. John, 'Intelligence Led Policing, Managerialism and Community Engagement: Competing Priorities and the Role of the National Intelligence Model in the UK' (2006) *Policing and Society* 16(1), 67-85, 67
[1331] Ibid
[1332] Ibid
[1333] M. Dawson, D. R. Kisku, P. Gupta, J. K Sing, W. Li, *Developing Next-Generation Countermeasures for Homeland Security Threat Prevention* (New York, IGI Global 2016) 87
[1334] Ibid

unavoidable, as without this it is impossible to deter cyber criminals and to sufficiently protect the public and the digital space in advance. The analysis of the UK cybercrime framework highlighted that it has whole-heartedly embraced the preventative policing approach, which relies heavily on intelligence gathering through mass surveillance. In contrast, a much more traditional policing style is still being pursued in the UAE. However, this is insufficient for the digital age, as also confirmed by the interviewees and the literature.

The failure to shift towards a new policing model is partly attributable to the fact that the UAE has not yet formally equipped law enforcement agencies with the requisite surveillance powers. Hence, one significant issue at present is that the UAE's surveillance system has not been sanctioned by law, which is a serious oversight in light of the planned expansion of its surveillance capabilities.[1335] Article 43 of Federal Law No. 5 of 2012 only provides a reactive surveillance power to law enforcement agencies, as opposed to a proactive one. In other words, the law does not permit that surveillance can be conducted prior to the commission of any offence, but only provides for this once offenders have been convicted. This is in marked contrast to the expansive and elaborate surveillance powers which, have been granted to many public bodies in the UK, as discussed in Chapter Three. The democratic basis is therefore lacking in the UAE to conduct mass surveillance through the use of technology, which can flag up suspicious activities. As a result, policing effectiveness is undermined since it is more difficult for law enforcement agencies to identify whether criminals, as well as spies and terrorists,

[1335] Saab, Saab receives order for new advanced airborne surveillance systems from UAE, 10 November 2015 <http://saabgroup.com/media/news-press/news/2015-11/saab-receives-order-for-new-advanced-airborne-surveillance-systems-from-uae/> accessed 28th April 2016

employ technologies to further their own objectives.[1336] Whilst it was pointed out by the interviewees that some surveillance takes place, it was acknowledged that without the enactment of a surveillance law issues also arise since this contravenes Article 31 of the UAE constitution, which guarantees the right to privacy. Without the enactment of a surveillance law, the UAE also opens itself up to accusations that the rule of law, as well as human rights are not afforded.

It is for these reasons that urgent recommendations are presented in this chapter, so that it is ensured that the e-policing approach is no longer reactionary but up to date with the latest technological advances. In this context, it must be emphasised that this particularly means utilising "big data" in order to identify potential high risk individuals.[1337] In other words, it necessitates that personal data is being collected on a mass scale, which in turn raises complex right to privacy issues.[1338] This also represents a much more technocratic policing approach i.e. one which is driven by quantitative assessments performed by computers and artificial intelligence programs.[1339] For instance, law enforcement agencies in the UAE, could use Clouderaa and Apache Hadoop software packages in order to analyse big data more effectively.[1340]

Having in mind that the UAE puts greater emphasis on the protection of privacy it is likely that the steps I propose will be heavily criticized, therefore it is important for any suggestion to carefully scrutinize the steps implemented as well as the proportionality of

[1336] C. A. Theohary, J. W. Rollins, Cyberwarfare and Cyberterrorism: In Brief, Congressional Research Services, 27 March 2015, 1-15, 2 <https://fas.org/sgp/crs/natsec/R43955.pdf> accessed 3rd September 2017

[1337] E. E. Joh, 'Policing by Numbers: Big Data and the Fourth Amendment' (2014) *Washington Law Review* 89, 35-68, 35

[1338] Ibid, 68

[1339] Ibid, 67

[1340] CTOlabs.com, 'White Paper: Big Data Solutions For Law Enforcement', June 2012, 1-8, 1 <https://theartofservicelab.s3.amazonaws.com/All%20Toolkits/The%20Big%20Data%20Solutions%20Toolkit/Act%20-%20Recommended%20Reading/Big%20Data%20Solutions%20For%20Law%20Enforcement.pdf> accessed 1st September 2017

using such steps. For example, the use of the steps may not be appropriate or even proportionate in all scenarios, therefore we would have to consider the scenarios in which such approach should apply, such as a 'ticking bomb' scenario[1341].

Even in the UK, where privacy is does not appear to be as paramount as in the UAE back in January the Court of Appeal ruled that the UK's DRIPA was inconsistent with EU law[1342]. Having in mind that the DRIPA has expired, as indicated above, the Court of Appeal's judgment is important with respect to current surveillance practices and it will have a major effect on the successor of DRIPA, the Investigatory Powers Act.

The DRIPA permitted access to communications data when the objective was not restricted solely to fighting serious crime. Additionally, the Court held that DRIPA lacked adequate safeguards since it permitted access to communications data without subjecting such access to a prior review by a court or independent administrative authority, having this in mind I am of the opinion that, with the appropriate safeguards and with clear guidelines as to when such approach may be used, my suggestions can be implemented in order to lead to an improved legal framework with respect to cybercrime.

The shift in the e-crime policing strategy must firstly be facilitated through the enactment of a comprehensive surveillance law, similar to the one which the UK has adopted in the form of the RIPA. This would ensure that the interception of communications is put on a statutory footing, as also strongly recommended by the interviewees. Such a law should spell out which bodies are granted the new policing powers. For example, the following provision could be adopted:

> *"(1) The military, the secret service, police and customs shall be permitted to intercept communications; conduct intrusive surveillance; require parties to decrypt data; use Covert Human Intelligence Sources; conduct directed*

[1341] S. Martin, (2016) 'Spying in a Transparent World: Ethics and Intelligence in the 21st Century' Geneva Papers, 19/16 Research Series.
[1342] *SSHD v Watson and Others* [2018] EWCA Civ 70.

surveillance and acquire communications data; conduct targeted hacking, subject to various safeguards.

(2) Etisalat and the Telecommunications Regulatory Authority shall acquire and intercept communications data and can require parties to decrypt data.

(3) The Dubai Financial Services Authority and the Abu Dhabi Global Market Financial Services Regulatory Authority are permitted to make decryption requests and can conduct intrusive surveillance.

(4) The powers spelled out in paragraphs (1)-(3) can be evoked by the various bodies if the Ministry of Interior or a federal judge has authorised this by signing a warrant or a court order either in advance or subsequently, except when the power has been used by the secret service and the military. In the latter case, it is sufficient that the Ministry of Defence is notified that any of these powers have been exercised."

Many of the interviewees also cautioned that mass surveillance is a double-edged sword since it fundamentally undermines the right to privacy. It is for this reason that it is advocated that only law enforcement agencies, the state-owned communications service providers and the entities in charge of overseeing the financial system should be equipped with these powers. This may prevent that powers are being overused by bodies. Otherwise, citizens may feel that their privacy is unduly interfered with, to the extent that they feel no longer safe from intrusion in their own homes, especially with

the introduction of smart-technology which can also be used for surveillance purposes.[1343]

It is also essential for each of these new types of powers to be clearly defined by the UAE surveillance law. An interception could be defined as follows:

> *"An interception takes place when a communication is accessed by someone who is not the recipient or sender of the communication. This can include instances where devices are bugged and hacked or contain technology which makes interception possible, including on a mass scale."*

The term 'communication' should be construed broadly, so that it includes content, stored data, such as voices and voice messages, subscriber information (e.g. the name of the subscriber and address details), service use information (e.g. information about who was called when and for how long, as well as how the web and social and phone media is used), as well as traffic data (e.g. information about the place from where the communication was sent).

However, the length of time during which these types of communications should be available to relevant agencies should be statutorily limited. Hence, data should be destroyed promptly after the particular investigatory purpose has been fulfilled. A failure to do so could constitute a criminal offence.

[1343] T. Timm, The government just admitted it will use smart home devices for spying, The Guardian, 9 February 2016 <https://www.theguardian.com/commentisfree/2016/feb/09/internet-of-things-smart-devices-spying-surveillance-us-government> accessed 2nd September 2017

The term 'surveillance' must also be statutorily defined, for example, as *"any action which is taken, including through any technological means, which results in the communications, activities, conversations or whereabouts of persons being listened to, observed or recorded."* A surveillance law ought to permit both intrusive and directed surveillance. Each type of surveillance should be defined, for instance, as:

> *"(a) An intrusive surveillance takes place when the private property of a person is being entered in order to install a device.*[1344]
>
> *(b) A directed surveillance takes place when a person's activities, conversations or movements are being monitored."*

The meaning of the term Covert Human Intelligence Sources should also be defined, as follows:

> *"Using an individual to create a relationship with someone in order to gain information or access information."*

The term decryption must also be explained in the proposed surveillance law, for example, in the following manner:

> *"Decryption means requiring those who can be suspected to have the key for an encrypted device to disclose this key so that the device can be accessed."*

[1344] D. Anderson, *A Question Of Trust* (London, Her Majesty's Stationery Office 2015) 143

Those empowered to make use of this decryption power should be expressly specified in the law. It must also be addressed what happens when there is a failure to comply with a request to provide a key or password: Firstly, it must be ensured that those requested to comply with a decryption request do not inform the password/key holder that they have provided access. This can be achieved by requiring them to sign an undertaking to that effect. Secondly, compliance must be promoted with decryption requests by rendering a failure to comply illegal. The applicable fine and sentence must therefore be stipulated by the surveillance law. A suspect who is required to provide a password, but who refuses to do so could receive a harsher sentence and/or fine. Hence, a refusal to comply with a decryption request by a defendant could be considered an aggravating factor. This would heighten deterrence. Additionally, law enforcement agencies could be permitted to conduct cyber-attacks in order to gain access to encrypted contents. Yet the latter leads down a slippery slope since it opens the door to abuse which is very difficult to monitor. However, this could be addressed by the above-mentioned safeguards which could apply to equipment interferences which could also be used to gain access to encrypted data.

When the national security of the UAE is also under threat, the secret service and military ought to be entitled to conduct targeted hacks. Put differently, they should be able to interfere with the equipment of cyber criminals, for example, when there is a suspicion that they plan to attack a vital infrastructure of the UAE, such as the soon to

be completed nuclear power station in Barakah. Such a provision could be worded as follows:

> *"The secret service and military can conduct equipment interferences in circumstances when there exists a reasonable suspicion that criminals or other rogue agents plan to attack the UAE or important infrastructure or to conduct acts of terrorism, subject to this having been authorised by the Ministry of Defence and a panel of specially appointed judges."*

Moreover, an oversight regime must be created when these different law enforcement powers are being evoked. The Ministry of Interior or a federal judge hearing cases in a secret court[1345] could be entitled to grant a warrant or approve the use of these powers through an authorisation or court order when this is necessary to protect the national security, to promote the economic well-being or to combat and investigate serious crime in the UAE. In the case of an equipment interference, oversight is best ensured through the Ministry of Defence and a panel of specially appointed judges.

A provision which contains a non-exhaustive list of the types of crimes which should be considered serious, such as attacking critical state infrastructure, ought to be also inserted into the surveillance law. In the alternative, any offence which attracts a sentence of at last three years could be considered serious, except in respect of equipment interferences for which a much higher threshold would have to be met.

[1345] W. W. Keller, *Democracy Betrayed: The Rise of the Surveillance Security State* (Berkeley, Counterpoint 2017) 43

The adoption of a provision in these terms ought to also contain a sub-paragraph with a proportionality and necessity requirement. In other words, the Ministry of Interior or a federal judge - or in the case of an equipment interference, the Ministry of Defence and the panel of specially appointed judges - should consider whether the requested power is necessary to realise the stated aim or goes above what is necessary. If the latter is the case, then a warrant or court order should only be issued for a less intrusive power. Yet when a warrant or court order is only sought subsequently, the power has already been exercised. In such instances, the Ministry of Interior or a federal judge ought to be entitled to impose certain conditions in respect of how the obtained evidence can be used if they deem this essential in order to protect the due process rights of the defendant.

A less stringent authorisation regime should be adopted for Covert Human Intelligence Sources, directed surveillance and the acquisition of communications data. This is because the intrusion is less severe than when intrusive surveillance takes place. A list should be drawn up of those public agencies which are granted these particular powers. A less stringent authorisation regime could be adopted. The head of the various public bodies could be empowered to approve use of these powers when this is important to safeguard national security; to preserve national unity; to protect the economy; to safeguard public health and safety; and for any other purpose approved by decree.

However, even the requirement to obtain a warrant or court order may not be sufficient to prevent that these far-reaching powers are not abused. This is because requests by law

enforcement agencies may just be rubber-stamped i.e. may never be denied. One way to overcome this issue is to further subject the surveillance regime to judicial oversight, as the case in the UK. In the UK, various commissioners have been appointed, as well as a tribunal. Such a set up ensures that abuse of powers and human rights are curtailed. The adoption of a surveillance law therefore also requires that a new office and tribunal are created, which is entrusted with overseeing that any surveillance law is being complied with and also in a way which complies with the rights conferred by the UAE constitution and the Sharia. This would go some way to create a checks and balances system.

Surveillance is only useful if data is also retained, as it is unrealistic to expect law enforcement agencies to immediately evaluate the information which is being obtained through the surveillance. It is for this reason essential that the topic of data retention is also addressed. The interviewees also agreed that data retention is of great importance in the detection of cybercrime. The UK has therefore adopted specific legislation which spells out the legal parameters of the data retention regime, as discussed in chapter three. However, as observed in chapter four, there exists no such law in the UAE. It is for this reason proposed that the Telecommunications Regulatory Authority issues regulations which impose a legal obligation to retain historical data, such as unsuccessful phone calls, IP addresses, email and location data, as well as how the web and social and phone media is used. Such data should be retained in an easily accessible format. Such a duty will help law enforcement agents to protect the *"national security, defence, public*

security or the prevention, investigation, detection, and prosecution of criminal offences of unauthorised use of the electronic communications system."[1346]

The telecommunications service provider Emirates Telecommunications Corporation (Etisalat), telecom operator Emirates Integrated Telecommunications Company (Du) and ISPs should therefore be required by law to retain data and to make it available to law enforcement agents when they request this. They would therefore have to retain data and could be sanctioned for a failure to ensure this. Hence, these organisations could be responsible for creating bulk personal datasets. These datasets could be further enriched through private and public partnerships, as further discussed below.

However, as access to this data violates Article 31 of the UAE constitution, it is important that access is not granted point blank. It should therefore be also rendered a criminal offence for employees of these organisations and unauthorised persons to unlawfully access retained data. Whilst Federal Law No. 5 of 2012 and Federal Law by Decree No. 3 of 2003 on Telecom Law can be construed to apply to these types of cases, it would be better to address these types of cases through a specific provision. For instance, a provision could be adopted which delineates that:

> *"Employees and others performing services for Etisalat, DU and ISPS and who have access to retained data are not allowed to access the retained data without being authorised. A breach of this provision attracts a minimum fine*

[1346] Article 15 of the now defunct European Union Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector; C. Walker, *Terrorism and the Law* (Oxford, Oxford University Press 2011) 75

of 18,000 AED and/or a minimum prison sentence of three months which in serious cases of unauthorised access can be extended to up to ten years."

However, a defence of an implied authorisation from a superior should be added. This would allow that those who merely follow instructions from superiors are not unfairly punished.

A special authorisation regime must also be detailed, which law enforcement agents would have to follow in order to request access. The access grounds could be to protect the national security, to promote the economic well-being or to combat and investigate serious crime. These could constitute objective criteria against which access grounds can be assessed. For instance, a request to investigate a traffic violation could not be justified. Additionally, it could be required that the access request is limited to a particular time period, restricted to a geographical area or an individual or particular group of individuals. However, access should be automatically provided when technology flags up suspicious conduct, which exceeds a certain threshold. Human feedback could be also given after cases have been automatically identified through data analysis software. This would help to assess to what extent the software is useful in combating cybercrime.

Exceptions must also be devised in urgent cases where cyber attacks pose the risk of loss of life, serious damage to national security, serious injury or illness. However, it

could be made a requirement to subsequently provide written justifications for the request.

It is recommended that no manual process should be used, but instead a technical platform appears better with a built-in procedure to make access requests. Each access request could thereby be permanently recorded on this platform and officers or artificial intelligence powered software could provide the reasons why access requests were sought.

A commissioner could be appointed at the Telecommunications Regulatory Authority with quasi-judicial functions and who could oversee the access requests and automatically flagged up cases. Such a commissioner would thus be in charge of scrutinising whether access is too-far reaching. The commissioner could issue guidance to law enforcement agents on how to use the power to access retained data and could award damages to individuals in case of serious privacy violations. Privacy undertakings could be imposed on those individuals who are being awarded damages in order to protect the work of law enforcement agencies. The commissioner could also be responsible for liaising with technology companies which make available the data analysis technology in case too many cases are being flagged up arbitrarily.

Law enforcement agencies responsible for serious breaches could also be fined and individual officers could be reprimanded. Such an approach would overcome some of the issue encountered with data retention in Europe where the Court of Justice of the

European Union declared the data retention regime unlawful. This was because the interference with privacy rights was disproportionate. In other words, by requiring that access requests are made and by examining who is flagged up automatically by technology, it is ensured that individuals do not have to fear that their entire private lives are constantly under surveillance or they are not unfairly identified as potential suspects. This is because retained data would not be accessed by law enforcement agents, except in specific cases where this is necessary and a proportionate response in relation to a suspected threat or crime. Furthermore, particular persons could be appointed from different public bodies and who could make these access requests or who receive the automatic software notifications about potential suspects. These individuals could be trained in privacy and data protection and anti-discrimination laws. This may go some way to ensure that access requests are not being abused and that technology does not result in unfair profiling of certain groups.

Moreover, the Telecommunications Regulatory Authority should carefully consider for how long data should be retained. In Europe, the length used to be set at six months and up to two years.[1347] In the UK, this was shortened to twelve months. The interviewees explained that a longer period is obviously more useful for law enforcement agents, though they also recommended to have regard to the data retention period which has been adopted by other countries.

[1347] C. R. Martin, S. L. Weakley, *Internet Law and Practice in California* (Oakland, CEB 2015) para.21.18A

Apart from these steps, a legislative debate must also take place since the internet of things makes it possible to spy on a much-larger scale than ever before.[1348] For instance, Samsung's Smart TV captures whatever users talk about in their homes through voice recognition technology and various other devices, such as Xbox Kinect, have built-in listening devices.[1349] This is a severe violation of the right to privacy and companies should not be allowed to collect such highly sensitive and private communications. Yet law enforcement agents may want to have access in appropriate cases. In other words, it is important that guidance is issued for companies which sell products with built-in listening devices, so that Article 31 of the UAE constitution is not violated.

It must also be addressed how it is ensured that law enforcement agencies have access to such communications, as such data is certainly extremely valuable to combat crime, including cybercrime. The question of whether foreign companies which sell these products within the UAE should be able to spy on UAE residents must also be discussed. Whilst the terms and conditions for these products may disclose that the devices are being used for these purposes[1350], it is debatable whether this complies with privacy rights. This is because these practices constitute an interception and so long as this is not sanctioned by law, it should constitute an offence pursuant to Federal Law No. 5 of 2012 and which cannot be circumvented through a contractual provision.

[1348] Ibid
[1349] Ibid
[1350] T. Timm, The government just admitted it will use smart home devices for spying, The Guardian, 9 February 2016 <https://www.theguardian.com/commentisfree/2016/feb/09/internet-of-things-smart-devices-spying-surveillance-us-government> accessed 2nd September 2017

Equally, it is important that privacy guidance is published for social media companies, such as Facebook, Instagram and Twitter, which analyse private data and use it for commercial purposes.[1351] Such an approach is important as frequently these social media companies work together with other companies, such as Geofeedia, a private company, which provides surveillance services available to over 500 US law enforcement bodies.[1352] Again whilst the terms and conditions to which users must agree may provide for this, such practices highlight that the right of privacy has become much more elusive in the digital age.

Yet in order to avoid criticism of unconstitutional law enforcement behaviour, it is important for the surveillance law to also address in which circumstances corporations can employ technology for surveillance purposes. One such condition should be that this is only done to assist law enforcement bodies. Access must also be restricted to law enforcement agents. In the EU, it was announced in May 2017 that the European Commission will spell out new powers for law enforcement officers, so that they can access even encrypted data, e.g. on WhatsApp. This may be achieved through legal rules, but also through the conclusion of private agreements between businesses and law enforcement agencies.[1353]

The surveillance law should therefore also permit law enforcement agencies to require private and public bodies to provide access to their data in real-time and to feed this into

[1351] D. Cameron, Dozens of police-spying tools remain after Facebook, Twitter crack down on Geofeedia, The Daily Dot, 11 October 2016 <https://www.dailydot.com/layer8/geofeedia-twitter-facebook-instagram-social-media-surveillance/> accessed 1st September 2017
[1352] Ibid
[1353] C. Stupp, EU to propose new rules targeting encrypted apps in June, 29 March 20017 <https://www.euractiv.com/section/data-protection/news/eu-to-propose-new-rules-on-police-access-to-encrypted-data-in-june/> accessed 1st September 2017

a data fusion centre.[1354] For example, the FBI employs data fusion i.e. feeds data from the private and public sector into one place in order to generate useful intelligence through big data analysis.[1355]

For this purpose, UAE law enforcement agents could enter into private and confidential agreements. However, such private sector cooperation must also be closely supervised. This is because technology is not error proof and arbitrary conclusions may be drawn which disadvantage certain individuals.[1356]

Law enforcement agents should therefore only access data in particular cases (e.g. when they investigate serious crime or this is necessary to protect the national security or the economy or public health), despite the fact that data is being collected about everyone. Technology would also alert them automatically when suspicious behaviour is being flagged up. The relevant provision in the surveillance law could be worded in the following terms:

> *(1) "The military, the secret service and police are empowered to gain access to data sets held by businesses and public bodies and which they can feed into a data fusion center.*

[1354] D. Lambert, 'Intelligence-Led Policing in a Fusion Center', Federal Bureau of Investigation, December 2010 <https://leb.fbi.gov/2010/december/intelligence-led-policing-in-a-fusion-center> accessed 1st September 2017

[1355] Ibid

[1356] Statewatch, 'Note on big data, crime and security: Civil liberties, data protection and privacy concerns, 3 April 2014, 1-6, 6 <http://www.statewatch.org/analyses/no-242-big-data.pdf> accessed 1st September 2017

(2) For these purposes, they can enter into private and confidential agreements in order to acquire or have access to data in real-time for intelligence-led policing purposes.

(3) These private and confidential agreements must be provided to the Ministry of Interior alongside a regularly updated list of those individuals which have been flagged up by intelligence software as high risk through the analysis of the various data sets.

(4) A special committee must be convened at the Ministry of Interior which is responsible for scrutinising on a regular basis whether those individuals which are identified as high-risk are being unfairly discriminated or denied any particular rights. Recommendations must be made to law enforcement agencies in cases of less favourable treatment which cannot be justified in the name of national security."

Such a provision would go some way to address criticism about the indiscriminate use of mass surveillance facilitated through *"big data approaches."*[1357]

Data transfer agreements should also be entered into with other countries, as cybercrime often takes place across borders. Otherwise, there exists the risk that cybercrime cannot be fully investigated, despite mass surveillance. As discussed, in chapter three the UK has operated a "worldwide spying network" through Echelon[1358] and recently adopted

[1357] Ibid, 1

[1358] S. Millar, R. Norton-Taylor, I. Black, Worldwide spying network is revealed, The Guardian, 26 May 2001 <https://www.theguardian.com/uk/2001/may/26/richardnortontaylor.ianblack> accessed 1st September 2017

the Investigatory Powers Act 2016, which further permits to intercept communications data worldwide.[1359] However, it is argued that such an approach would be inappropriate for the UAE since it interferes with the sovereignty of other nations. It is therefore recommended that the better approach is to enter into data transfer agreements or treaties with other countries in order to obtain data, except in extremely serious, but isolated cases where an equipment interference is necessary in order to protect the national security of the UAE. The enactment of surveillance powers also requires that the relationship with the constitutionally guaranteed right to privacy is clarified, as discussed in the following section.

6.2 Privacy, Data Protection and Security

One fundamental problem is that surveillance powers interfere with the right to privacy and data protection. 'O'Leary argues that '[t]he risk of abuse is considered inherent in any system of secret or mass surveillance and such systems clearly interfere with rights to privacy and data protection'[1360]. However, by adopting a statutory regime which also contains various safeguards, it can be ensured that privacy and data intrusions are minimised. In other words, mass interception and surveillance by itself may not breach privacy and data protection rights, so long as law enforcement officers access data in limited cases where this is a proportionate and necessary response in order to combat crime or to ensure public security. This is because the right to privacy is no absolute

[1359] J. Vincent, The UK now wields unprecedented surveillance powers - here's what it means, The Verge, 29 November 2016 <https://www.theverge.com/2016/11/23/13718768/uk-surveillance-laws-explained-investigatory-powers-bill> accessed 1st September 2017
[1360] S. O'Leary (2018) 'Balancing rights in a digital age' Irish Jurist, 59, 59-92.

human right.[1361] As discussed in Chapter Four, like the UK, the UAE guarantees the right to privacy by virtue of Article 31 of the constitution, Article 378 of the Federal Law 3 of 1987 (Penal Code) and Article 21 of Federal Decree Law No. 5 of 2012 on Combating Cybercrimes and to a lesser extent affords data protection rights, though mainly in respect of entities which operate in the Dubai International Financial Centre. Yet Federal Law No. 5 of 2012 fails to state what is meant by 'privacy.' In contrast, the analysis of the UK legal framework showed that much more legal guidance exists in order to interpret the right to privacy, so that this right is less elusive than in the UAE.

Furthermore, whilst Articles 372 and 373 of Federal Law No.3 of 1987 (the penal code) require that it is shown that a defendant had an intention to cause harm or to disclose private information, this is not required by Federal Law No. 5 of 2012. It is also not clear how the constitutional right to privacy in Article 31 of the UAE should be interpreted in the context of e-crimes. One issue which can arise as a result of this is that harmless social media posts are being caught by Federal Law No. 5 of 2012 and result in criminal convictions.[1362] This is because Article 21 criminalises

> *"(1) Eavesdropping, interception, recording, transferring, transmitting or disclosure of conversations or communications or audio or visual materials.*
> *(2) Photographing others or creating, transferring, disclosing, copying or saving electronic photos.*

[1361] E. Claes, A. Duff, S. Gutwirth, *Privacy and the Criminal Law* (Oxford, Intersentia 2006) 74
[1362] Clifford Chance, The right to privacy online in the UAE - To post or not to post? Briefing Note, February 2016, 1-3, 2

(3) Publishing news, electronic photos or photographs, scenes, comments, statements or information even if true and correct."

As it has become a normal occurrence to record and photographs and to publish such media on sites, such as Facebook, it appears that the provision is too far-reaching in scope and can be used to convict innocent individuals. Another issue is that merely photographing others, even without publication, constitutes an offence.[1363] For instance, a person who takes a selfie in a public space and also photographs a third person may open him/herself up to potentially being prosecuted for a criminal offence. This is a too draconian approach which creates legal uncertainty. It is desirable that the *mens rea* requirement in the penal code is extended to Article 21 of Federal Law No. 5 of 2012. This would ensure that Article 21 has no overreach. In the alternative, it could be considered whether breaches of the right to privacy should be decriminalised. In other words, a violation of the human right to privacy would only result in the award of civil remedies. If such a stance was favoured, it would be important to remove the privacy provisions from Federal Law No. 5 of 2012. Such clarifications may also help to ensure that the right to privacy is more aligned with that of Western states.

Apart from sufficiently clarifying and fleshing out the concept of privacy, personal data and data protection, another challenge for UAE courts and academics is to develop the requisite jurisprudence in the context of balancing privacy against security interests. One way to commence the debate about the right to privacy and security would be to amend Article 31 of the UAE constitution. This Article currently provides that *"[f]reedom of*

[1363] Ibid

communication by means of the posts, telegraph or other means of communication and their secrecy shall be guaranteed in accordance with the law." However, it is unclear to what extent adoption of a law can abrogate the right to freely communicate in secret.

In contrast, Article 8 of the European Convention on Human Rights is more elaborate since sub-paragraph 2 not only mandates that any interference must be in accordance with the law, but also *"necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."* This provides a better yardstick for judges to balance privacy rights against security interests. It would therefore be useful if an additional caveat similar to that contained in Article 8(2) of the ECHR was added to Article 31 of the UAE constitution. However, security should not be viewed as the ultimate trump card, as it otherwise may promote the creation of a totalitarian regime. The interviewees also cautioned against mass surveillance becoming the 'new normal', as this effectively means no longer guaranteeing the human right to privacy. Instead, the starting point should be that the right to privacy, as well as the right to liberty and security constitute two equally important human rights.[1364] One important consideration which UAE judges should take into account when balancing privacy rights against security interests, is to consider how serious an offence is.[1365] Arguably, only serious offences justify that the

[1364] S. Stalla-Bourdillon, J. Phillips, M. D. Ryan, *Privacy vs. Security* (London, Springer 2014) 65
[1365] Ibid

right to privacy is being interfered with.[1366] For instance, when the offence is cyber terrorism then it is clearly a proportionate response to interfere with the personal privacy of the suspect.[1367] This is because public security it at stake. However, the same appears not to be a proportionate response in the case of harassment where surveillance does not appear justified. Apart from considering whether the procedural safeguards spelt out in any surveillance law have been complied with, as well as the seriousness of the offence, UAE judges should also consider how sensitive the personal data is which has been collected.[1368]

Moreover, the literature review in Chapter One highlighted that the UK's data protection regime is much more far-reaching than in the UAE. All entities which collect personal data must comply with the Data Protection Act 1998. As a result, businesses are legally compelled to safeguard personal data. In this way, privacy and data protection are reconciled with cyber security.[1369] This is also the case because data processing exceptions have been created for the police and judiciary.[1370]

In contrast, in the UAE individuals have not been afforded data protection rights and remedies, except when breaches have been committed in respect of credit information or by financial institutions which operate in the DIFC, as identified in Chapter four. The concept of data protection should therefore be developed. The interviewees also strongly

[1366] Ibid
[1367] Ibid
[1368] Ibid
[1369] M. G. Porcedda, Data Protection and the Prevention of Cybercrime: The EU as an Area of Security? EUI Working Papers, 2012/25, 1-90, 5 <http://cadmus.eui.eu/bitstream/handle/1814/23296/LAW-2012-25.pdf?sequence=1&isAllowed=y> accessed 3rd September 2017
[1370] Article 5 of Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters

recommended that the topic of data protection should receive more attention. This is because data protection and cyber security are "*two sides of the same coin.*"[1371] For the UAE, this means firstly extending the existing data protection law which applies to the Dubai International Financial Centre to the UAE as a whole. Such an approach would also close one of the current gaps highlighted by the interviewees, namely that data collection by companies is unregulated. This in turn is likely to indirectly promote digital security and may thereby reduce the occurrence of cybercrime. However, exceptions should be stipulated for law enforcement agents, but which are not excessive, so that that private and personal data is safeguarded, but without this adversely affecting policing operations.

Additionally, law enforcement agents could adopt a privacy policy, as recommended by the interviews. This may help to ensure that the various surveillance powers are not used in a way which marginalises the right to privacy and data protection. Communications service providers could report breaches within 24 hours to the Telecommunications Regulatory Authority and inform data subjects about the privacy and/or personal data breach. In turn, the Telecommunications Regulatory Authority could immediately alert law enforcement agencies about the security breach, which may help to avert cybercrime which may be perpetrated with the private and personal data from the security breach. This may help law enforcement agents to take preventive and pre-emptive steps.

[1371] V. Reding, The EU's Data Protection rules and Cyber Security Strategy: two sides of the same coin, European Commission, 2013 <http://europa.eu/rapid/press-release_SPEECH-13-436_en.htm> accessed 30 June 2014

Whilst these legal reforms are undoubtedly imperative, the right to privacy could also strengthened by a regulatory requirement which mandates that organisations employ "privacy enhancing technologies." [1372] Privacy-enhancing technology safeguards personal identity through organisational structures and technology, such as encryption, spyware and virus protection, privacy policies, anonymous proxies. [1373] Such a technocratic requirement could be phased in and firstly be imposed on organisations which deal with sensitive personal data.[1374] In other words, citizens' privacy could be protected through regulatory technical guidelines and standards. [1375] This is likely to result in a shift in approach by businesses which engage in data mining or which manufacture interception technologies. [1376] This is because they are currently not incentivised to protect privacy. [1377] However, by imposing a legal or regulatory requirement that devices, e.g. with built-in listening devices, such as SmartTVs, have privacy enhancing technologies embedded, they would be compelled to internalise privacy.[1378] Surveillance capacity could thus become curtailed through technological and legal restrictions, which in turn will help to respect the human right to privacy, as well as the related right to data protection.[1379] The governing principles on which such restrictions could be built is that of minimal data retention, data minimisation and

[1372] B. Akhgar, B. Brewster, *Combatting Cybercrime and Cyberterrorism: Challenges, Trends and Priorities* (London, Springer 2016) 286
[1373] C. Fuchs, K. Boersma, A. Albrechtslund, M. Sandoval*, Internet and Surveillance: The Challenges of Web 2.0 and Social Media* (Abingdon, Routledge 2012) 20
[1374] B. Akhgar, B. Brewster, *Combatting Cybercrime and Cyberterrorism: Challenges, Trends and Priorities* (London, Springer 2016) 286
[1375] European Central Bank, Forum on the Security of Retail Payments - SecureRe Pay, 2017 <https://www.ecb.europa.eu/paym/pol/forum/html/index.en.html> accessed 2nd September 2017
[1376] B. J. Goold, D. Neyland, *New Directions in Surveillance Privacy* (Abingdon, Routledge 2009) 29
[1377] Ibid
[1378] Ibid
[1379] Ibid, 30

"minimal data sharing and processing" i.e. data sharing in accordance with a "legally justifiable purpose."[1380]

Edgar also argues that people often wrongly agree that privacy must be sacrified in order to achieve security, but observes that such a conclusion is only reached because people "are not aware of privacy-enhancing technology" which can "mitigate such trade-offs."[1381] By adopting a private sector online identity management system with inbuilt privacy safeguards cybersecurity monitoring (i.e. mass surveillance) becomes less of a controversial topic.[1382] Practically, this means creating an online identity akin to a passport or identity card and no longer making use of passwords, so that online transactions are confirmed by a robust identity assurance.[1383] This will help to increase privacy and security. One crucial recommendation is therefore for the UAE legislator to create a digital identity for UAE citizens and residents. For example, the Swiss town of Zug recently announced that it will provide digital identities for its residents through an app which "secures personal information using blockchain technology and associates it with a crypto address."[1384] Such an approach would also accord with the latest trends in cyber security, as presented at the Digital Identity Summit which took place this

[1380] Ibid, 31
[1381] T. Edgar, 'The US Privacy Strategy' in (eds) D. Aspinall, J. Camenisch, M. Hansen, S. Fischer-Hubner, C. Raab, *Privacy and Identity Management, Time for a Revolution?* (London, Springer 2016) 20
[1382] Ibid, 21
[1383] Ibid, 27
[1384] B. Vitaris, Swiss "Crypto Valley" to Create Digital Identities for Its Citizens on the Ethereum Blockchain, Bitcoin Magazine 13 July 2017 <https://bitcoinmagazine.com/articles/swiss-crypto-valley-create-digital-identities-its-citizens-ethereum-blockchain/> accessed 3rd September 2017

September in San Francisco and will take place in Paris in 2018.[1385] Digital identity can also facilitate e-government services of which policing is one.[1386]

As of the 25th of May 2018 data protections changes in the UK and in the EU in general, as the EU General Data Protection Regulation ("the GDPR') enters into force, *'The GDPR is designed to protect and empower all EU citizen's data privacy, and to reshape the way organisations across the region approach data privacy. Following the UK's departure from the EU, the GDPR provisions will be retained in UK law by cl 3 of the European Union (Withdrawal) Bill, which incorporates EU law into domestic law. To give effect to the GDPR, the Government introduced the Data Protection Bill 2017 ("the Bill') into the House of Lords on 13 September 2017. Domestically, this legislation will replace the Data Protection Act 1998.'*[1387]

The first commentaries published with respect to the newly implemented regulation are far from positive, arguing that '*The regulation does little to change the way cookies monitor us on a site. You'll be tracked and manipulated just like before*.' [1388]

6.3 Federal Law No. 5 of 2012 Concerning Combating Information Technology Crimes

Overall the interviewees thought that Federal Law No. 5 of 2012 ensures that most cybercrime offences are covered. The analysis of Federal Law No. 5 of 2012 also

[1385] Digital Identity Summit 2017, The Currency of Trust, 2017 <https://digitalidentitysummit.com/> accessed 2nd September 2017

[1386] M. Ienco, Digital identity as a key enabler for e-government services, Mobile Connect, 2016, 1-8, 1 <https://www.gsma.com/identity/wp-content/uploads/2016/02/MWCB16-Digital-Identity-as-a-Key-Enabler-for-eGovernment-Services-Marta-Ienco.pdf> accessed 1st September 2017

[1387] -- (2018) 'Legislative Comment: Data Protection Bill 2017', Immigration, Asylum and Nationality Law 32(2) 98-99.

[1388] M. Dixon, (2018) 'GDPR should have made cookies toast', Fortune, <http://fortune.com/2018/05/24/gdpr-data-privacy-cookies/> accessed 22 June 2018.

showed that many different types of acts are outlawed. Yet some Articles are rather broad in scope, namely Articles 2, 4, 5, 8 and 9, as no distinction is drawn between using off-shore virtual private network (VPN) and hacking. Use of VPNs should not attract the same sentence, as hacking since the latter is clearly a much more serious offence. It should also not be deemed illegal to record a conversation, but instead a more nuanced approach should be adopted. In other words, consent should constitute a defence when a person records another or the circumstances are such that it appears warranted to make a recording, e.g. when a person possesses no men rea to commit a criminal offence.

Another issue with Federal Law No. 5 of 2012 is that the provisions, e.g. Articles 20, 28 and 29, are vague and far-reaching and as a result, they can be applied in a way which contravenes free speech. Guidance should be issued, so that lawful criticism can be distinguished from unlawful defamation. In this context, it is also noteworthy that the UN Special Rapporteur called on states not to use criminal sentences for defamation, but to instead employ civil law, as for instance, the UK does.[1389] The legislator should therefore consider decriminalising defamation and to consider this a civil case for which damages can be sought, as opposed to imposing criminal sanctions.[1390] Otherwise, the criticism that free speech is under attack may likely persist, which may not help to ensure that a progressive image is fully created.[1391]

[1389] Human Rights Council, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Mr Abid Hussain, E/CN.4/2001/64 (Annex V)
[1390] L. Langer, *Religious Offence and Human Rights: The Implications of Defamation of Religions* (Cambridge, Cambridge University Press 2014) 206
[1391] Human Rights Watch, UAE: Cybercrimes Decree Attacks Free Speech, 28 November 2012 <https://www.hrw.org/news/2012/11/28/uae-cybercrimes-decree-attacks-free-speech> accessed 1st September 2017

Moreover, Chapter Four also identified that Article 47 of Federal Law No. 5 of 2012 only confers extra-territoriality when a cybercrime is directed against the state. As this greatly diminishes the effectiveness of the cybercrime provisions, it is important that Article 47 is revised, so that it ensured that all crime is considered a local matter.[1392] This would also align Federal Law No. 5 of 2012 with Article 23 of the Penal Code which allows the Public Prosecutor to institute criminal proceedings against a person who commits a crime in a foreign country.

In the alternative, a threshold amount could be stipulated and certain offences could be classified as serious, so that in these instances the concept of extra-territoriality would apply automatically. However, as observed by the interviewees extra-territoriality also requires cooperation from other states. One way to signify that the UAE affords cooperation to other states would be to make clear that UAE nationals can be prosecuted for cybercrimes even if they do not reside in the UAE and the offence is one which the UAE also criminalises, despite it not being directed against the UAE. The analysis of the UK legal framework showed that such an approach has been adopted.[1393]

Yet this alone is insufficient and extradition treaties must also be entered into with other countries, particularly those in which many cybercrime criminals reside, in order to ensure that the extra-territoriality concept is not only a theoretical concept. However, it is unlikely that countries will extradite persons for matters which are not considered

[1392] R. Broadhurst, P. Grabosky, *Cyber-Crime: The Challenge in Asia* (Hong Kong, Hong Kong University Press 2005) 154

[1393] S.5(1a) and (1B) of the Computer Misuse Act 1990

criminal, especially defamation cases and privacy breaches. This further supports the above recommendation to remove defamation and privacy violations from Federal Law No. 5 of 2012. Otherwise, it could be made clear that extradition cannot be sought for these types of cases i.e. these cases should not pass the requisite threshold to be considered sufficiently serious to warrant extradition. This is because it is unlikely that these types of extradition requests will be granted.

Moreover, Federal Law No.3 of 1987 (the penal code) requires that crimes are notified and it would be useful for Federal Law No. 5 of 2012 to also contain a provision which requires businesses and organisations to notify cybercrimes in excess of a certain threshold. This alongside a requirement for communications service providers to report data protection breaches within 24 hours to the Telecommunications Regulatory Authority and to inform data subjects about the privacy and/or personal data breach, as recommended above, may ensure that the topics of cybercrime and cyber security receive more attention by enforcement agents.

Another deficiency of Federal Law No. 5 of 2012 is that it does not outlaw intellectual property crime. This kind of crime can be perpetrated through copyright infringement, piracy and counterfeiting of patents and trademarks.[1394] For instance, operating websites to advertise counterfeit goods or pirated software and movies could be criminalised. Organised criminals are particularly involved in this very lucrative market which takes

[1394] B. Zagaris, *International White Collar Crime: Cases and Materials* (2nd ed, Cambridge, Cambridge University Press 2015) 623

place on an enormous scale.[1395] Interpol has therefore also created a special contact point to assist law enforcement agents.[1396] As the UAE has been identified as one of the "main hubs for fake trade"[1397] this would be a further stepping stone to address this issue. Also, as software piracy (i.e. unlicensed software) particularly renders organisations and individuals more vulnerable to cybercrime since it often contains malware, this would also be another measure to combat cybercrime.[1398]

Another limitation of Federal Law No. 5 of 2012 is that there is no specific crime for launching cyber attacks against critical infrastructure. Contrariwise, the UK has adopted such a provision.[1399] It would be better if a provision was added which specifically covers situations where computers are impaired in order to cause serious damage or the risk of serious damage to UAE's national security, the economy, the environment or human welfare of private and state-owned critical infrastructure. UAE academics and professionals also support such a recommendation.

6.4 The Criminal Procedure Law and Procedural Rules Governing Electronic Evidence

The analysis of the Criminal Procedural Law Federal Law No. 35 of 1992 in Chapter Four showed that it is inadequate for the digital age. This is because there exist no

[1395] Ibid
[1396] Ibid
[1397] K. Megget, Hong Kong, Singapore and UAE main hubs for fake trade, Securing Industry, 23 June 2017 <https://www.securingindustry.com/hong-kong-singapore-and-uae-main-hubs-for-fake-trade/s111/a4881/#.Wbxc89HTXIU> accessed 2nd September 2017
[1398] J. Gassen, E. Gerhards-Padilla, P. Martini, 'Botnets: How to Fight the Ever-Growing Threat on a Technical Level' in (eds) H. Tiirmaa-Klaar, J. Gassen, E. Gerhards-Padilla, P. Martini, *Botnets* (London, Springer 2013) 45
[1399] S.3ZA of the Computer Misuse Act 1990

special procedural rules for electronic evidence, investigative, measures, third party cooperation duties, jurisdiction and international cooperation.[1400] However, at the regional level Articles 22 to 29 of the Arab Convention on Combating Information Technology Offences 2010 spell procedural rules, but these have not yet been fully transposed.

It is therefore crucial that this oversight is urgently remedied. Firstly, standard procedures for the collection, preservation and presentation of electronic evidence are required, so that evidence is not declared inadmissible.[1401] As discussed in chapter three, in the UK the National Police Chiefs' Council (NPCC) has published the Good Practice Guide for Digital Evidence, the Good Practice Guide for Computer-Based Electronic Evidence and the Good Practice Guide for Managers of E-Crime Investigation. Similarly, UAE police should promulgate guidelines which spell out the relevant technical procedures for digital evidence, computer-based electronic evidence and those who conduct investigations with an e-crime element. At the core of these guidelines should be to ensure that data is not changed, but kept intact.[1402] This must also be guaranteed when original data is being accessed by law enforcement agents.[1403] Officers must therefore be able to explain and testify that their actions have not affected the

[1400] K. A. Aljneibi, The Regulation of Electronic Evidence in the United Arab Emirates: Current Limitations and Proposals for Reform, PhD Thesis, February 2014, 1-326, 194 <http://e.bangor.ac.uk/4992/1/Aljneibi%20khaled%20thesis.pdf> accessed 15th February 2017; United Nations Office on Drugs and Crime, Approaches in national cybercrime legislation and the UNODC Cybercrime Repository, undated 1-44, 2 <http://unctad.org/meetings/en/SessionalDocuments/Cybercrime%20Nayelly%20Loya%20(UNODC).pdf > accessed 1st September 2017

[1401] K. M. Hess, C. H. Orthmann, H. L. Cho, *Police Operations: Theory and Practice* (6th ed, Boston, Cenage Learning 2013) 375

[1402] The Association of Chief Police Officers Good Practice Guide for Digital Evidence 2012, 1-43, 7 <http://www.acpo.police.uk/documents/crime/2011/201110-cba-digital-evidence-v5.pdf> accessed 2 May 2014

[1403] Ibid

data.[1404] All steps which have been taken must be clearly documented through an audit trial, so that other persons can verify what has been done.[1405] Responsibility for ensuring that the data has not been changed and to document the steps taken must rest with the person in charge of conducting the investigation.[1406] This would help with ensuring that evidence is not declared inadmissible at trial.[1407]

Moreover, the Criminal Procedure Law should contain provisions which permit that law enforcement agents can preserve stored data on digital devices and can require that it is not being changed or destroyed.[1408] Courts must also be empowered to order persons or organisations to preserve such data without any alteration for a stipulated time period. At present, Article 41 of Federal Law No. 5 of 2012 only provides that the court can order *"the confiscation of devices, programs or means used in the commission of any of the crimes."* Hence, no power exists which legally mandates not to alter data.

Traffic data must also be preserved and promptly made available to competent law enforcement agencies or individuals responsible for cybercrime investigations.[1409] A new section which enables the court to make a production order should also be inserted in the Criminal Procedure Law.[1410] Such a provision would make it possible to order those in control or possession of specific computer data, including service providers, to make data available to the relevant authorities. Additionally, the person or organisation

[1404] Ibid
[1405] Ibid
[1406] Ibid
[1407] Ibid
[1408] Articles 23-24 of the Arab Convention on Combating Information Technology Offences 2010; also see Article 16 of the Council of Europe Cybercrime Convention
[1409] Also see Article 17 of the Council of Europe Cybercrime Convention
[1410] Article 26 of the Arab Convention on Combating Information Technology Offences 2010; also see Article 18 of the Council of Europe Cybercrime Convention

which receives such an order must be required not to disclose such a request. Hence, a type of tipping off offence must be included, so that suspects are not alerted.

New powers must also be conferred on law enforcement agents to conduct electronic searches and seizures.[1411] Such search and seizure powers must extend to keeping copies but without compromising the integrity of the data, as well as removing or making inaccessible the data in appropriate cases. However, the search and seizure power is only effective if relevant organisations or persons can be ordered to safeguard the data.

It must also be possible to compel telecommunication services and social media companies, such as Facebook, to gather and record data and to assist and co-operate with law enforcement agents in real-time.[1412] Access points must therefore be provided and private and confidential agreements must be entered into, so that this is facilitated, as also suggested above. Service providers must therefore be statutorily obligated to assist with the interception of data.[1413] Whilst Etisalat and Du are closely connected to the government and there therefore does not exist a pressing need, in the digital age important data is also held by many other organisations, especially on mobile devices and apps, such as WhatsApp. It is for this reason important to enact a power which can be extended to these other operators, so that vital evidence is not being hidden from the competent authorities. Law enforcement agencies should discuss with the legislator

[1411] Article 27 of the Arab Convention on Combating Information Technology Offences 2010; also see Article 19 of the Council of Europe Cybercrime Convention
[1412] Article 28 of the Arab Convention on Combating Information Technology Offences 2010; also see Article 20 of the Council of Europe Cybercrime Convention
[1413] Article 29 of the Arab Convention on Combating Information Technology Offences 2010; also see Article 21 of the Council of Europe Cybercrime Convention

which service providers should provide real-time access, so that interception can take place. Clearly, those services which are very popular, such as Facebook, WhatsApp, Skype, should be obligated to provide real-time access.

Special rules are also needed when electronic evidence has been obtained through surveillance.

The analysis of the UK evidence rules highlighted that government secrets can be protected through the concept of public interest immunity.[1414] No such concept exists in the UAE and as a result intelligence sources may be disclosed to the defendant during criminal court proceedings. In light of the fact that the UAE intends to increase its surveillance capability, sensitive information should be similarly protected. A legislative procedure should therefore be developed, so that the prosecutor can make an application in relevant cases to protect the sources and investigatory techniques of law enforcement agencies. Yet judges cannot simply grant such applications, but must carefully assess the documents in respect of which confidentiality is sought. This is because non-disclosure of evidence contravenes notions of fairness and arguably breaches the right of the defendant to have a fair hearing. Hence, it must be in the public interest to grant an order which prevents a defendant to see certain documents. In the UK, this is normally granted when national security requires this, to safeguard anonymous informers and also for covert surveillance operations.[1415] Intercepted communications are also covered by

[1414] C. Forsyth, 'Public Interest Immunity: Recent and Future Developments' (1997) 1 *Cambridge Law Journal*, 51-59, 51

[1415] *Rogers v Secretary of State for the Home Department* (1973) AC 388; *D v NSPCC* (1978) AC 171

public interest immunity.[1416] The UAE could adopt the following legal provisions and insert them in the Criminal Procedural Law Federal Law No. 35 of 1992:

> *"(1) The prosecutor must provide the accused with any material, including material which weakens the case of the prosecution, except when public interest immunity is successfully pleaded by the prosecutor.*
>
> *(2) In case, public interest immunity is asserted by the prosecutor, an application must be made to the court to determine this. For this purpose, the judge must balance the right of the accused to have a fair hearing against the public interest, namely to ensure national security, safeguard anonymous informers and covert surveillance operations and prevent disclosure of intercepted communications, except when the sender or receiver of the intercepted communication has expressly consented to the interception.*
>
> *(3) The prosecutor is barred from making a public interest immunity application when this clearly undermines the fairness of the legal proceedings.*
>
> *(4) The court can order the prosecution to admit a specific fact when this is deemed important to guarantee the fairness of the hearing for the accused."*

Nevertheless, the various measures outlined are not enough if cooperation is lacking; steps must be taken to strengthen this area as discussed next.

[1416] S.17 of RIPA

6.5 Cooperation

As cybercrime is borderless, it is crucial that countries cooperate with each other to bring perpetrators to justice. The interviewees also emphasised that international and regional co-operation is an absolute priority in order to combat cybercrime effectively. Article 23 of the Council of Europe Cybercrime Convention also emphasises that co-operation should take place "to the widest extent possible." The interviewees suggested that the UAE should actively lobby for a UN-based cybercrime treaty. Yet in the absence of such a treaty, it is essential that co-operation is established with law enforcement agencies from all around the globe. For this purpose, a memorandum of understanding could be drawn up which spells out the terms of cooperation, including in respect of undertaking joint cybercrime investigations. For instance, Europol has increased internet security and cybercrime cooperation through such a memorandum of understanding.[1417]

The UAE could also enter into mutual legal assistance treaties with other countries which particularly cover cybercrime offences. Either one of these methods would ensure that legal obligations are detailed on how to assist with cybercrime investigations, as well as prosecutions. Expertise and assistance could be pledged, as well as information disclosure. A special department could be created at the Ministry of Interior, which could be in charge of entering into these memoranda of understanding with foreign authorities and mutual legal assistance treaties with other countries.

[1417] Europol, 'Europol enhances cybercrime and internet security cooperation by signing MOU with EURID', 21 December 2016 <https://www.europol.europa.eu/newsroom/news/europol-enhances-cybercrime-and-internet-security-cooperation-signing-mou-eurid> accessed 1st September 2017

In the absence of such memoranda of understanding or mutual legal assistance treaties, co-operation should also be promoted through diplomatic channels, as also mentioned by the interviewees. Law enforcement agents would submit details, e.g. through the Ministry of Interior, to the embassy of the particular state in question from which cooperation is sought, so that it is then passed on to the relevant law enforcement agencies.[1418] Yet this channel is often slow[1419] and may therefore not be as effective at bringing cyber criminals to justice. This is because a request does not impose an international legal duty on the state to which it is made, whereas this is the case with mutual legal assistance treaties.[1420] However, even mutual legal assistance treaties do not ensure that requested evidence is promptly provided.[1421]In case a foreign country is not a party to any multilateral treaty which provides judicial assistance, UAE courts could also make more use of letters rogatory i.e. could formally request a foreign court to render judicial assistance, e.g. to provide evidence.[1422] However, such letters do not compel the other country to comply with any request.[1423]

Another means to heighten cooperation is for the UAE to enter into extradition treaties. An extradition treaty creates a legally binding obligation on the state parties to transfer an accused who resides in one country to the other. Such an extradition treaty could list

[1418] J. D. McClean, *International Co-operation in Civil and Criminal Matters* (Oxford, Oxford University Press 2002) 16
[1419] Ibid
[1420] S. W. Brenner, *Cybercrime: Criminal Threats from Cyberspace* (Santa Barbara, Greenwood Publishing Group 2010) 143
[1421] Ibid
[1422] J. R. Westby, *International Guide to Combating Cybercrime* (Chicago, ABA Publishing 2003) 45
[1423] Ibid

the particular offences in relation to which an accused can be extradited.[1424] However, it is better for the extradition treaty not to list the offences as cybercrime constantly evolves and this risks that cyber criminals escape their punishment because of an omission to include a particular offence. Instead, it is better to include a clause which makes clear that extradition can be sought so long as both states punish the offence for at least one year.[1425] Whilst Article 24 of the Council of Europe Cybercrime Convention stipulates in respect of which offences extradition can be sought, it also makes clear that they must attract a minimum punishment of at least one year. Equally, Article 31 of the Arab Convention on Combating Information Technology Offences 2010 states that the offence must result in the *"deprivation of freedom for a minimum period of one year or a more severe penalty."*

An authority must also be created which is responsible for extradition or procedural arrests.[1426]

Yet even when there exists an extradition treaty, it may be legally challenging to ensure that a suspect is transferred.[1427] All of these different channels which promote cooperation should nonetheless be pursued, despite their limitations. Police forces, as well as individual investigators should additionally engage in informal cooperation i.e. should network with colleagues in other countries.[1428]

[1424] Ibid, 46
[1425] R. Broadhurst, P. Grabosky, *Cyber-Crime: The Challenge in Asia* (Hong Kong, Hong Kong University Press 2005) 275
[1426] Article 31(7)(a) of the Arab Convention on Combating Information Technology Offences 2010
[1427] S. W. Brenner, *Cybercrime: Criminal Threats from Cyberspace* (Santa Barbara, ABC-Clio LLC 2010) 145
[1428] Ibid

Yet co-operation whether through agreements, treaties, formal or informal requests or diplomatic channels depends on the country having procedural and substantive laws in place.[1429] Whilst the UAE has substantive laws in place, it must also develop the requisite procedural laws, as discussed above. Procedural laws must also be enacted in order to facilitate international cooperation and mutual assistance. This includes requests by foreign states to "*obtain the expeditious safeguarding of information stored on an information technology located within its territory"*[1430] and *"users tracking information related to specific communications",*[1431] as well as *"to investigate, access, seize, secure or disclose the stored information technology information located within the territory."*[1432]It should be statutorily mandated that UAE law enforcement authorities furnish information, even without being requested to do so, to another law enforcement authorities in circumstances when they consider that this may assist the foreign law enforcement authority.[1433] Such information should be made available subject to the condition that it must be kept confidential or any other specific conditions.

Furthermore, the UAE must develop the capacity so that mutual assistance requests can be rapidly and efficiently answered.[1434] It must also create the necessary mechanisms to facilitate requests on a twenty-four-hour basis every day of the week.[1435] Practically, this

[1429] S. Schjolberg, *The History of Cybercrime: 1976-2014* (Norderstedt, Cybercrime Research Institute GmbH 2014) 122
[1430] Article 37 of the Arab Convention on Combating Information Technology Offences 2010
[1431] Article 38 of the Arab Convention on Combating Information Technology Offences 2010
[1432] Article 39 of the Arab Convention on Combating Information Technology Offences 2010
[1433] Article 33 of the Arab Convention on Combating Information Technology Offences 2010; Article 26 of the Council of Europe Cybercrime Convention
[1434] Article 32 of the Arab Convention on Combating Information Technology Offences 2010; S. Schjolberg, *The History of Cybercrime: 1976-2014* (Norderstedt, Cybercrime Research Institute GmbH 2014) 122.
[1435] Ibid (Schjolberg)

means setting up a Cybercrime Cooperation Department, which is responsible for dealing with requests from foreign agencies.[1436] Such a department could act as central contact point for foreign authorities which seek assistance with cybercrime investigations. Such requests should only be refused in cases where it is considered that the offence is a political one or where the sovereignty, ordre public, security or any other important interest is adversely affected.[1437] The requisite technological platform must also be created, as well as a streamlined procedure through which requests can be made by foreign partners. Expert personnel and resources must be made available to this department.

Formal and informal cooperation mechanisms must thus be developed.[1438] National capacity must be developed i.e. law enforcement agents, the judiciary and prosecutors must receive cybercrime training.[1439]

This chapter has illustrated how the research findings have contributed to knowledge creation, through the gathering and analyses of theoretical information and empirical evidence. As a result, the final two chapters of the thesis will address how the research objectives have been met and present the recommendations.

[1436] Articles 34 and 43 of the Arab Convention on Combating Information Technology Offences 2010; Article 27 of the Council of Europe Cybercrime Convention
[1437] Article 27(4)(a)-(b) of the Council of Europe Cybercrime Convention
[1438] United Nations Office on Drugs and Crime, Approaches in national cybercrime legislation and the UNODC Cybercrime Repository, undated 1-44, 2 <http://unctad.org/meetings/en/SessionalDocuments/Cybercrime%20Nayelly%20Loya%20(UNODC).pdf > accessed 1st September 2017
[1439] Ibid

7. Conclusion

A critical comparison of e-crime legislation in the UK, EU and UAE has uncovered many conflicting and often problematic dichotomies incorporating safety in the digital realm and mass surveillance, the public and private interest, proactive and reactive regulatory measures, privacy and intrusion, protecting civil liberties and infringing upon them, to name a few. This study has shown how these conflicting aspects continue to provoke controversy and spark debate amongst lawmakers, academics, politicians, law enforcement, human rights groups and the general public. As extensively depicted in the research, all legislation is closely aligned with the political aims and economic priorities of a country, region or group, yet this comparative study which incorporates the UAE legislative framework that is shaped by Sharia law, has foregrounded some of the ways that legislation is driven and circumscribed by dominant cultural, religious and social norms and agendas.

The key areas covered in the research were primarily laws regulating cybercrime, surveillance, data retention, data protection and privacy in the UK, EU and UAE. The admissibility of electronic evidence and intercepted communications in criminal court proceedings and non-disclosure (and the public interest) were an integral part of the analysis. The research was comprised of an empirical element for triangulation of the research data, and to contribute to a more textured understanding of the research topic.

Five senior experts in the field of cybercrime from the UAE were interviewed, representing the judiciary, the police, Interpol, the office of prosecution and the Telecommunications Regulatory Authority. Taken all together, these theoretical and empirical resources were utilised to comprehensively assess the existing legislation in the UAE and consider ways that it might be improved.

To meet the research aim and objectives key e-crime legislation and other associated laws issuing from the UK, EU and UAE were analysed and incorporated:

The seminal legislation adopted by the UK to deal with cybercrime offences, namely, the Computer Misuse Act 1990. It has proved instrumental in prosecuting perpetrators of cybercrime offences due to its very wide scope. Authorisation and unauthorised acts performed on a range of electronic devices with the capacity to store data, as well as intent to access data are incorporated in the Act and due to the way in which they are loosely defined, it has been effectively used to cover an extensive range of cybercrime offences. The Serious Crime Act 2015, which was constituted as an amendment to the 1990 Act has been criticised for its ill-defined concepts such as 'damage to human welfare' which carry sentences of life imprisonment.

The thesis explored the UK surveillance and UK and EU data retention laws. Laws which govern surveillance and data retention underpin an effective legislative framework to combat e-crime. Nevertheless, intrusive surveillance and covert investigation techniques in the UK which were based on the EU Data Retention

Directive (2006/24/EC) and deemed essential by law enforcement agencies, were found to be in breach of the Human Rights Act 1998 and the European Court of Human Rights. Owing to this, the UK's Regulation of Investigatory Powers Act 2000 (RIPA) and Terrorism Act 2000 were pivotal in legalising interception, intrusive surveillance, data acquisition and decryption. Moreover, intrusive techniques sanctioned by RIPA can and are being used by hundreds of other bodies, authorities and companies. Many find it concerning that they are being monitored and reviewed internally, and not independently.

An analysis of the UK Data Retention (EC Directive) Regulations 2009 in the thesis revealed that it was deemed to be controversial for failing to clarify what crimes (with the exception of organised crime and terrorism) would necessitate data retention. This was a major oversight since this regulation allowed the retention of data for an inordinate amount of time. It was thought that this regulation could succumb to abuse by authoritarian regimes and constitute an erosion of human rights and a violation of the privacy rights of citizens. It was explained in the thesis that the scope and application of legislations such as these must be clearly defined and safeguards imposed. The Data Retention and Investigatory Powers Act 2014 (DRIPA) and the Investigatory Powers Act 2016 were adopted in response to the Court of Justice of the European Union ruling that the 2009 Data Retention Directive was invalid.

Another important strategy to combat cybercrime is to ensure that steps are taken to protect the right to privacy, especially personal data. This makes it more difficult for

cyber criminals to utilise this data for criminal purposes. Privacy, data protection and network and information security laws are intrinsic to strengthening e-crime legislation. The thesis examined the UK and EU privacy and data protection, and network and information security laws. It showed how the Human Rights Act 1998 and Article 8 of the ECHR were in accord with each other. They both stipulate that the right to privacy shall not be interfered with by a public authority, except in accordance with the law, democratic society, national security, public safety and the prevention of disorder or crime. The UK Data Protection Act 1998 and the Directive 96/46/EC protect the rights to privacy with regard to the processing of personal data. Businesses who collect personal data must comply with this legislation. The UK Act has been updated by a new Data Protection Bill which was published in the UK in September 2017. The bill aims to overhaul the existing UK data protection to reflect an increasingly digital age and economy. The Directive 96/46/EC has also been replaced and updated by the General Data Protection Regulation to harmonise and strengthen data protection for people in the EU, it will apply from May 2018.

When cyber criminals are being prosecuted, it must also be ensured that digital evidence is not declared inadmissible and criminal evidence rules must be in place, including for intercept material. Otherwise, cases may be thrown out or the work of law enforcement agencies may be undermined. Addressing these matters therefore also forms part of an effective legislative strategy to combat cybercrime. The UK evidence rules on the admissibility of digital evidence and intercept material in criminal proceedings were analysed in the research. What constitutes evidence obtained by illegal and unfair

means which cannot be relied upon in court? The answer to this question is chiefly determined by the RIPA. Unauthorised and/or intrusive surveillance is inadmissible if it is RIPA evidence. It is acknowledged that justice and the public interest is a difficult balance to achieve or balancing administration of justice against non-disclosure. The issue is disclosure of police work and covert information to organised crime networks.

Turning to the UAE, the thesis critically evaluated the effectiveness of its legislative framework to combat e-crime. Comparatively, the UAE is a newcomer, its first cybercrime law, the Federal Law Decree No. 2 of 2006 was enacted nearly two decades after the UK. It was replaced with **Federal Legal Decree No. 5 for 2012** and **Federal Legal Decree Law No. 3 of 2012** was also adopted to establish the National Electronic Security Authority. Federal Law No. 2 of 2006 was specifically formulated to combat identity theft, internet fraud, hacking and harm caused to the public. Article 16 illustrated some of the issues with these UAE laws. It declares it to be illegal to breach family values and principles or to publish anything which invades the privacy of another person or their family life. Yet it does not define 'family values and principles' or what 'private information' is deemed to be. Further, this article renders surveillance of the digital realm illegal and did not include a provision for enforcement agencies to circumvent it. In comparison to the proactive methods of RIPA in the UK, the UAE does not have a surveillance law and its work in this area is reactive. Surveillance is restricted to monitoring web content which contravenes UAE's moral and ethical code, such as pornography, gambling, illegal drugs and religious hatred. In contrast to the UK, there is also no legislation that covers data retention and very little that seriously

addresses data protection. The exception concerns situations where there is a data protection breach associated with credit information or financial services connected to the Dubai International Finance Centre (DIPC).

The successor to No. 2 of 2006 was Federal Law No. 5 of 2012. It was seen as an improvement for delineating more cybercrime violations, removing the need to demonstrate intent, dealing with the issue of authorisation and access, and for covering a wide range of online websites. It increased data protection for e-payment services and online data. Additionally, stricter penalties, higher fines, deportation of offending foreigners and sentences up to seven years were imposed. It was found to be more comprehensive, but there were still legislative gaps and inefficiencies. Once again the area of privacy has proven problematic. The increase of privacy violations as detailed in the 2012 law potentially voids some of the cybercrime violations and once again restricts surveillance by law enforcement agencies. In comparison, the UK legal framework contains clear legal guidance in the interpretation of privacy rights.

In addition, the above UAE laws were analysed in the research through the lens of senior and experienced experts in the UAE from the Department of Cybercrime, the Fujairah Federal Court of First Instance, the General Directorate of Investigations at Dubai Police, the Dubai Public Prosecution and the Telecommunications Regulatory Authority. They acknowledged the need for legislation which regulates the processes and procedures for e-crime prevention, investigations and prosecutions. Laws currently not covered were identified as those for surveillance, data protection, data retention,

decryption requests and law enforcement. It was felt that legislation needs to keep pace with new technology and criminal behaviour, whilst balancing privacy rights with security interests so that mass surveillance does not become normalised. Data transfer agreements with other countries on a par with Europol, were viewed as essential in combating e-crime.

With respect to research design, the second chapter explained the methodology, namely the ontology, epistemology, research philosophy, research design, approach to analysis. Reasons were provided why a mixed method research approach - consisting of doctrinal legal analysis/the black letter law approach and the comparative method, as well as empirical qualitative research - was chosen. Accordingly, it was discussed how the positivist approach was supplemented by the interpretative stance in the form of a qualitative segment i.e. interviews with different key stakeholders from the UAE. As a result of the empirical research, it was necessary to consider how sensitive issues should be addressed and how ethics can be maintained. The qualitative interviewing techniques which were used were described, as well as the sampling procedure. Moreover, the setting of the interviews was outlined, as well as the method of recording and how data quality was achieved. Additionally, it was explicated how the data was analysed, as well as the approach to publish the qualitative research.

The research also contributed to knowledge creation. The e-crime legislation in the UAE was analysed in a comprehensive manner. Federal Law No. 5 of 2012 concerning combating information technology crimes was analysed holistically. Put differently, it

was considered that a mere legal analysis of the cybercrime offences is insufficient to strengthen e-crime legislation in the UAE. The horizon was widened by making recourse to other jurisdictions, namely the UK and the EU. The research provided novel insights since UK and EU e-crime laws served as comparators. The evaluation of the UK and EU e-crime laws particularly highlighted the importance of shifting towards a more proactive policing style facilitated by surveillance and data protection, strong privacy and data protection rights, as well as clear procedural criminal procedure laws for electronic evidence. New legislative recommendations could be developed based on the UK and EU legal frameworks. These were more refined than if only the UAE e-crime legislation had been analysed.

Hence, a much broader range of aspects which affect the effectiveness of cybercrime policing was considered. The question of how to strengthen e-crime legislation in the UAE was thus not confined to the narrow legislative toolbox of merely criminalising certain acts. An innovative and inclusive research strategy was thus pursued.

Very little research had been conducted to analyse Federal Law No. 5 of 2012 concerning combating information technology crimes. Moreover, this is the first piece of legal research which not only analyses e-crime legislation in the UAE, but which also takes into account the views of senior and experienced e-crime experts in the UAE. The question of whether e-crime legislation has been effective was therefore better understood. Broader descriptions were obtained which looked at the phenomenon of cybercrime and its intricacies.

The in-depth doctrinal research was thus supported through the qualitative part of the research and information which is different to a theoretical legal analysis. Such an approach was also useful since UAE legal cases are not normally published and are only occasionally reported in the media. As the UAE only enacted its first piece of e-crime legislation in 2006 there still exists very little research in this area. This research therefore contributes to the literature in the UAE and may be a useful reference point for academics and practitioners alike.

The research has distinct advantages and also some limitations. An in-depth legal analysis was conducted as primary e-crime legislation was studied. Legal gaps, contradictions, ambiguities and other limitations within the statutory provisions and available laws in the UAE were identified. Other issues which impede the effectiveness of the e-crime framework were pointed out. However, one limitation is that the analysis of the UAE e-crime laws in chapter four does not refer to as many cases as chapter three, the doctrinal analysis of the UK e-crime legislation, as well as EU law. This made it difficult to know how the different offences in Federal Law No. 5 of 2012 are being interpreted. However, this was not an insurmountable problem since as a judge the researcher is aware of the typical judicial approaches employed.

Moreover, the research sample was rich in quality, as senior and experienced UAE experts were interviewed. Certainly, it would have been desirable to also interview

experts from the UK. Ideally, it may have been also useful to employ a questionnaire and to distribute it to a large sample. However, as this is not a social science thesis, such a research strategy was not chosen. The underlying reason for this is also that doctrinal legal research is rooted in positivism. Laws can be objectively ascertained and distributing questionnaires may therefore not have added much additional information.

Another benefit of this research was that the e-crime legislation in the UAE was studied against the backdrop of the UK and EU laws, which directly and indirectly combat cybercrime. Hence, the Western approach towards combating cybercrime was taken into account and these new insights helped with the development of new legislative solutions for the UAE. Of course, even more insights would have been gained had recourse been made to even more jurisdictions. More improvement suggestions could have been generated. Although studying several different jurisdictions would have risked that the e-crime laws in respective jurisdictions are not properly investigated.

The fact that the research was limited to the UAE, UK and EU also does not mean that the research was not comprehensive. On the contrary, a benefit of this research was that a variety of different types of legislation were evaluated and the topic of strengthening e-crime legislation was analysed holistically. It is conceded that more emphasis could have been placed on each specific definition contained in Federal Law No. 5 of 2012 had the focus been on scrutinising the cybercrime offences in the UAE. However, such an approach was not adopted as it was considered that merely criminalising certain acts as cybercrime is insufficient to secure the digital space. Surveillance, data retention,

privacy and data protection laws and criminal procedure laws which govern electronic evidence were therefore studied. Certainly, each of these topics could fill several books. Nevertheless, the clear advantage of such an approach was that it made it possible to identify key aspects of different types of legislation which underpin an effective legislative e-crime framework.

However, even these topics are not the only tools to fight cybercrime; legislation is only one discipline amongst many. Human resource management, forensics and software, technology and design development are other areas which can greatly contribute to combating cybercrime. Nonetheless, it would have been inappropriate to consider them here, as this was explicitly a law-centred, driven and focused research project.

8. Recommendations

As set out at the beginning of the thesis, a key aim of the research is to contribute to knowledge creation by assisting UAE legislators to strengthen e-crime legislation. By drawing together the theoretical and empirical resources of this study, this chapter identifies and delineates provisions in order to show where they can be amended, revised, supplemented or completely discarded. Additionally, draft provisions are proposed therein which can form the backbone of e-crime legislative reform in the UAE. If such recommendations are enacted they may assist other countries in the Middle East to combat cybercrime more effectively.

1. A preventative and intelligence-led policing model

a) Fundamentally, the UAE must move towards a more preventative and intelligence-led policing model.
b) A surveillance law must be urgently enacted. Such a law must equip law enforcement agents with various powers, particularly to intercept communications; conduct intrusive surveillance; require parties to decrypt data; use Covert Human Intelligence Sources; conduct directed surveillance and acquire communications data; and conduct targeted hacking.
c) As some of these powers are more intrusive, it should be ensured that only certain public bodies can make use of these powers.

d) Legal safeguards must also be put in place to prevent abuse of powers. It could be required that a warrant is granted or a court order is obtained.

e) Additionally, an oversight regime should be created and for this purpose a commissioner could be appointed with quasi-judicial functions at the Telecommunications Regulatory Authority and a specialised tribunal could be set up.

2. A data retention law to facilitate data access for law enforcement agents

a) A data retention law must also be enacted, which obligates Etisalat, Du and ISPs to retain data and to make it available to law enforcement agents when they request this.

b) A data retention period of one year appears reasonable.

c) Access should only be granted to authorised persons in cases where certain access grounds – i.e. to protect the national security, to promote the economic well-being or to combat and investigate serious crime – are made out.

d) Data retention by the private sector can also provide important clues for cybercrime investigations. Law enforcement agents should therefore also be empowered to enter into private agreements, so that they have access in real time to other data, such as social media posts and WhatsApp messages. Such data could then be fed into an intelligence data fusion center.

e) In the near future, it should be studied how the UAE can create an intelligence data fusion center i.e. what model they should adopt to enhance information

sharing.[1440] As data gathering is at the heart of surveillance and data retention, future research must also be conducted about the privacy implications of *"individual intelligence profiles"* which are thereby created.[1441]

3. Heightening privacy and data protection

a) Cyber security can be heightened, especially if data protection legislation was adopted throughout the UAE. As the ultimate objective is to combat cybercrime, privacy and data protection should be viewed as "*two sides of the same coin."*[1442]

b) The right to privacy as guaranteed in the constitution should be further developed. This is particularly important to facilitate that privacy rights can be better balanced against security interests.

c) Communications service providers should also be required to report breaches within 24 hours to the Telecommunications Regulatory Authority. This may help to avert cybercrime.

d) A regulatory requirement which mandates that organisations employ *"privacy enhancing technologies"*[1443] could also be imposed.

e) Most importantly, the UAE should consider creating digital identities for its citizens and residents, including corporate entities. [1444] New blockchain

[1440] W. E. Smith, Developing a Model Fusion Center to Enhance Information Sharing, PhD Thesis, Naval Postgraduate School, Monterey, California, December 2011, 1-115, 1 <http://www.dtic.mil/dtic/tr/fulltext/u2/a556626.pdf> accessed 3rd September 2017

[1441] T. Mendel, A. Puddephatt, B. Wagner, D. Hawtin, N. Torres, *Global Survey on Internet Privacy and Freedom of Expression* (Paris, United Nations Educational, Scientific and Cultural Organization 2012) 46

[1442] V. Reding, The EU's Data Protection rules and Cyber Security Strategy: two sides of the same coin, European Commission, 2013 <http://europa.eu/rapid/press-release_SPEECH-13-436_en.htm> accessed 30 June 2014

[1443] B. Akhgar, B. Brewster, *Combatting Cybercrime and Cyberterrorism: Challenges, Trends and Priorities* (London, Springer 2016) 286

[1444] World Economic Forum, A Blueprint for Digital Identity, The Role of Financial Institutions in Building Digital Identity, World Economic Forum, August 2016, 1-108, 1

technology could be employed, such as the civic secure identity platform, which offers individuals and businesses to protect and control their identities.[1445] Alternatively, the UAE could create a *"universal national digital identity scheme using blockchain"* technology like Estonia has set up.[1446] This could help protect user's privacy, whilst at the same time helping to bring down cybercrime, especially digital identity crime.[1447]

f) Research must therefore be also conducted on how to create digital identity systems, including with the help of blockchain technology.[1448] Future research should also explore what impact such technology has for policing in a surveillance age.

4. Improving Federal Law No. 5 of 2012 concerning Combating Information Technology Crimes

a) Federal Law No. 5 of 2012 concerning Combating Information Technology Crimes should be further improved.

b) The concept of extraterritorial jurisdiction in Article 47 should be expanded.

<http://www3.weforum.org/docs/WEF_A_Blueprint_for_Digital_Identity.pdf> accessed 1st September 2017; B. Vitaris, Swiss "Crypto Valley" to Create Digital Identities for Its Citizens on the Ethereum Blockchain, Bitcoin Magazine 13 July 2017 <https://bitcoinmagazine.com/articles/swiss-crypto-valley-create-digital-identities-its-citizens-ethereum-blockchain/> accessed 3rd September 2017

[1445] Civic.com, 2017 <https://www.civic.com/> accessed 1st September 2017

[1446] M. Mainelli, Blockchain will help us prove our identities in a digital world, Harvard Business Review, 16 March 2017 <https://hbr.org/2017/03/blockchain-will-help-us-prove-our-identities-in-a-digital-world> accessed 1st September 2017

[1447] A. Faulkner, How to Use Anonymized Global Digital Identities to Fight Cybercrime, RSA Conference, 8 April 2016 <https://www.rsaconference.com/blogs/how-to-use-anonymized-global-digital-identities-to-fight-cybercrime> accessed 1st September 2017

[1448] M. Mainelli, Blockchain will help us prove our identities in a digital world, Harvard Business Review, 16 March 2017 <https://hbr.org/2017/03/blockchain-will-help-us-prove-our-identities-in-a-digital-world> accessed 1st September 2017

c) An additional provision which outlaws attacks on critical infrastructure should be inserted.

d) A provision which specifically criminalises digital IP crime should be added to Federal Law No. 5 of 2012.

e) A notification requirement for businesses and organisations for certain threshold cybercrimes may prove useful. It would put pressure on the public and private sector to adopt sufficient security measures to combat cybercrime. A notification requirement would also help with the development of cybercrime statistics, which should include information about the number of prosecutions and successful convictions. This is important for studying how effective the e-crime legislation has been in bringing criminals to justice.

5. Revision of the Criminal Procedural Law Federal Law No. 35 of 1992 and adoption of additional guidelines

a) The Criminal Procedural Law Federal Law No. 35 of 1992 must be revised.

b) An additional part should be added for electronic evidence.

c) The Council of Europe Cybercrime Convention and the Arab Convention on Combating Information Technology Offences could serve as base for the development of new cybercrime procedures, including powers.

d) Additionally, the police should develop guidelines for digital evidence, computer-based electronic evidence and those who conduct investigations with an e-crime element. In this context, research should also be conducted about the

best digital investigation processes.[1449] Research must also be continuously conducted about cybercrime trends.[1450]

6. Enhancing regional and international cooperation

a) Efforts must be made to enhance international and regional cooperation, particularly through the conclusion of extradition treaties and mutual legal assistance treaties, but also other channels, including informal ones.

[1449] United Nations Office on Drugs and Crime, Approaches in national cybercrime legislation and the UNODC Cybercrime Repository, undated 1-44, 2 <http://unctad.org/meetings/en/SessionalDocuments/Cybercrime%20Nayelly%20Loya%20(UNODC).pdf > accessed 1st September 2017
[1450] Ibid

9. Bibliography

Treaties

Arab Convention on Combating Information Technology Offences 2010

Council of Europe Convention on Cybercrime 2001

European Convention on Human Rights 1950

Regional Instruments

European Union Charter of Fundamental Rights

EU Laws

Commission Regulation 611/2013 of June 2013 on the measures applicable to the notification of personal data breaches under Directive 2002/58/EC of the European Parliament and of the Council on privacy and electronic communications

Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union [2005] O.J. C197

Council Decision of February 28, 2002 [2002] O.J. L63

Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems

Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters

Council Directive 97/66 of the European Parliament and of the council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector

Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data

Data Retention (EC Directive) Regulations 2007 (SI 2007/2199)

Declaration 21 on the protection of personal data in the fields of judicial and police cooperation in criminal matters

Directive 2002/59 concerning the processing of personal data and the protection of privacy in the electronic communications sector

Directive 2013/40/EU on attacks against information systems

Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union

Directive on privacy and electronic communications (2002/58/EC)

Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector

Directive 95/46 on the protection of individuals with regard to processing of personal data and on the free movement of such data

Directive 2006/24/EC on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC

Draft European General Data Protection Regulation 2012

Council of Europe Recommendation No. R (87) 15 regulating the use of personal data in the police sector (2002)

Council Recommendation on contact points maintaining a 24-hour service for combating high-tech crime [2001] O.J. C187

Electronic Communications (EC Directive) Regulation 2003

European Union's Framework Decision on attacks against information systems

European Union Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data

European Union Directive 2002/58 on Privacy and Electronic Communications

European Union Directive 2009/136 of the European Parliament and of the Council

Framework Decision on Police and Judicial Cooperation in Criminal Matters

Data Retention Directive (2006/24/EC)

General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679)

Regulation 460/2004 of the European Parliament and of the Council establishing the European Network and Information Security Agency (Text with EEA relevance) [2004] O.J. L077/1-11

Treaty of Lisbon 2007

Treaty on the Functioning of the European Union

United Nations Draft Resolutions

Commission on Crime Prevention and Criminal Justice, *Draft resolution: strengthening international cooperation to combat cybercrime*, UN ESCOR, 22nd sess., Agenda Item 7, UN Doc E/CN.15/2013/L.14 (2 April 2013) 2

UAE Statutes

UAE Cabinet Resolution No. 21 of 2012 concerning Information Security Regulations in the Federal Authorities

UK Counter-Terrorism and Security Act 2015

UK Criminal Procedure and Investigations Act 1996

UAE Criminal Procedural Law Federal Law No.(35) of 1992

UAE Dubai International Financial Centre Law No.5 of 2005

UAE Dubai Healthcare City Regulation No.7 of 2008

UAE Dubai International Financial Centre Data Protection Law No.1 of 2007

UAE Executive Council Resolution No.13 of 2012 regarding the Information Security in the Government of Dubai

UAE Federal Law No.15 of 1980 Governing Publications and Publishing

UAE Federal Law 3 of 1987 the Penal Code

UAE Federal Law No. 37 of 1992, as amended by Law No. 19 of 2000

UAE Federal Law No. 7 of 2002 in respect of author copyright and parallel rights

UAE Law No.8 of 2002 concerning Trade Marks

UAE Federal Law No. 17 of 2002, as amended by Federal Law No. 31 of 2006 concerning the protection of industrial property law

UAE Federal Law No. 3 of 2003 Regarding the Organisation of Telecommunications Sector, as amended by Federal Law No.5 of 2007 regarding the regulation of Etisalat and the communications sector

UAE Federal Law No.2 of 2006 on combating cybercrime

UAE Federal Law No. 3 of 2012 on establishing the National Electronic Security Authority

UAE Federal Law No. 5 of 2012 concerning combating information technology crimes

UAE Federal Law No.15 of 1980 on printed matter and publications

UAE Law No.2 of 2015 concerning Commercial Companies

UK Statutes

UK Anti-Terrorism Crime and Securities Act 2001

UK Computer Misuse Act 1990

UK Copyright, Designs and Patents Act 1998 Terrorism Act 2006

UK Criminal Attempts Act 1981

UK Criminal Damage Act 1971

UK Criminal Justice Act 1988

UK Criminal Procedure Rules 2011

UK Criminal Procedure and Investigations Act 1996

UK Data Protection Act 1998

UK Data Retention and Investigatory Powers Act 2014

UK Digital Economy Act 2010

UK Disorder Act 1998

UK Forgery and Counterfeiting Act 1981

UK Human Rights Act 1998

UK Intelligence Services Act 1994

UK Interception of Communications Act 1985

UK Investigatory Powers Act 2016

UK Malicious Communications Act 1998 Telecommunications Act 1984

UK Obscene Publications Act 1959 and 1964 Protection of Children act 1978

UK Police Act 1997

UK Police and Criminal Evidence Act 1984

UK Police and Justice Act 2006

UK Post Office Act 1969

UK Prison Act 1952

UK Protection from Harassment Act 1997

UK Protection of Children Act 1978

UK Protection of Freedoms Act 2012

UK Public Order Act 1986 and Crime

UK Regulation of Investigatory Powers Act 2000

UK Regulation of Investigatory Powers (Communications Data) Order 2010 (SI 480/2010)

UK Regulation of Investigatory Powers (Extension of Authorisation Provisions: Legal Consultations) Order 2010 (SI 2010/461)

UK Serious Crime Act 2007

UK Serious Crime Act 2015

UK Sexual Offences Act 2003

UK Terrorism Act 2000

UK Terrorism Act 2006

UK Wireless Telegraphy Act 2006

Cases

UAE Federal Supreme Court case, Supreme No. 10/2011

UAE Federal Supreme Court case, Supreme No. 50/2011

UAE Federal Supreme Court case, Supreme No. 185/2011

UAE Federal Supreme Court case, Supreme No. 165/2012

UAE Federal Supreme Court case, Supreme No. 120/2013

UAE Federal Supreme Court case, Supreme No. 345/2013

Guidance

UK Communications Data Code

UK Serious Crime Act 2015, Explanatory Notes
<http://www.legislation.gov.uk/ukpga/2015/9/notes> accessed 1st December 2015

UK Serious Crime Bill, Explanatory Notes, 2014, 1-85

<http://www.publications.parliament.uk/pa/bills/lbill/2014-2015/0001/en/15001en.pdf>

accessed 20th January 2015

UK Parliamentary Debates

Hansard, HC Debs 15 July 2014, Col 714 (Theresay May) and Co 723 (Yvette Cooper)

UK Cases

A v Secretary of State for the Home Department (No.2) [2005] 3 WLR 1249

A-G's Reference (No.1 of 1991) (1993) QB 94

AG v Guardian Newspapers (No 2) [1990] AC 109

AJA and Others v Metropolitan Commissioner (2014) 1 All ER 882

Al Rawi v Secretary of State for the Home Department (2011) UKSC 34

Air Canada v Secretary of State for Trade (No.2) [1983] 2 AC 394

Al Rawi v Security Service [2011] UKSC 34

Atkins v DPP [2000] 2 All ER 425

Burmah Oil Co Ltd v Bank of England [1980] AC 1090

Chambers v Director of Public Prosecutions [2012] EWHC 2157 (Admin); [2013] 1 WLR 1833

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

Conway v Rimmer [1968] AC 910

Cox v Riley (1986) 83 Cr App R 54

D v NSPCC (1978) AC 171

DPP v Bignell (1998) 1 Cr App R 1

DPP v Lennon (2006) 170 JP 532

DPP v McKeown; DPP v Jones (1997) 1 WLR 295

Duchess of Argyll v Duke of Argyll [1967] Ch 302

Durant v Financial Services Authority [2003] E.W.C.A. Civ. 1746

Edwards v UK [2003] 15 BHRC 189

Fox v Chief Constable of Gwent [1985] 3 All ER 392

Gatland v Commisioner of Police of the Metropolis [1968] 2 WLR 1263

Goodridge v Chief Constable of Hampshire Constabulary (1999) 1 All ER 896

Halford v UK (1997) 24 EHRR 523

Jeffrey v Black [1978] QB 490

Johnson v Medical Defence Union (MDU) [2005] 1 W.L.R. 750

Jones v Owen [1870] 34 JP 759

Jones v University of Warwick [2003] EWCA Civ 151

Kopp v Switzerland (1999) 27 EHRR 91

Kuruma Son of Kaniu v R [1955] AC 197

Liberty [2014] UKIPTrib 13_77-H

Malone v Metropolitan Police Commissioner (No.2) [1979] Ch 344

Marks v Beyfus [1890] 25 QBD 494

Michael Douglas v Hello! Ltd (No. 2) [2003] EWHC 786 (Ch)

R.v P [2002] 1 AC 146

Paton v Poole Burgh Council, Unreported July 29, 2010 (IPT)

Re C's Application for Judicial Review [2009] UKHL 15; [2009] 1 AC 908

Re McE [2009] UKHL 15

R v Allsop (2005) EWCA Crim 703

R v Aujili (1998) Cr App R 16; *R v X, Y and Z*, The Times, 23 May 2000

R v Austin (2009) EWCA Crim 1572

R v Bedworth (unreported) 1991

R v Bow Street Magistrates Court Ex p. Allison [1999] 4 All ER 1

R v Clowes [1992] 3 All ER 440

R v Coulson and another (2013) EWCA Crim 1026

R v Cox and Railton (1884) 14 QBD 153

R v Cropp (unreported) 4 July 1990

R v Davis [1993] 1 WLR 613

R v E (2004) 1 WLR 2379

R v Effick (1995) 1 AC 309

R v Fellows and Arnold [1997] 2 All ER 484

R. v Gold [1988] AC 1063

R v Governor of Brixon Prison, ex parte Osman [1992] 1 All ER 108

R v Horseferry Road Magistrates' Court, ex p Bennett [1993] 3 All ER 138

R v Khan [1996] 3 WLR 162

R v Khan (Sulton) [1997] AC 558

R v Lambert [2002] AC 545

R v Latif, R v Shahzad [1996] 1 All ER 353

R v Leatham [1861] 8 Cox CC 498

R v Lindesay (2002) 1 Cr App R (S) 270

R v Looseley and Attorney General's Reference (No.3 of 2000) [2001] 1 WLR 2060

R v Maxwell [2010] UKSC 48

R (on the application of NTL Group Ltd) v Ipswich Crown Court (2002) EWHC 1585

R v Parr-Moore (2003) 1 Cr App R (S) 425

R v Preston (1994) 2 AC 130

R v Quinn [1990] Crim LR 581

R v Shivpuri (1987) AC 1

R v Smurthwaite and Gill [1994] 1 All ER 898

R v Talboys, The Times 29 May 1986

R v Turner (Elliott Vincent) [2013] EWCA Crim 642

R v Whitaker (1993) unreported (Scunthorpe Magistrates' Court)

Rogers v Secretary of State for the Home Department (1973) AC 388

Sargent [2003] 1 AC 347

Schenk v Switzerland (1988) 13 EHRR 242

Smith v Lloyd TSB Bank Plc [2005] W.L. 636009

SSHD v Watson and Others [2018] EWCA Civ 70

*Stephens **v** Avery* [1988] FSR 510

Wainwright v Home Office [2003] 3 WLR 1137

Warren v Attorney General for Jersey [2011] UKPC 513

European Court of Human Rights Cases

Amann v Switzerland, App. No.27798/95, Judgment of February 16, 2000

Copland v United Kingdom (2007) 45 EHRR 37 ECtHR

Edwards and Lewis v United Kingdom (2005) 40 EHRR 24

Friedl v Austria (1996) 21 EHRR 83 ECtHR

Halford v United Kingdom (1997) 24 EHRR 523 ECtHR

Khan v United Kingdom (2001) 31 EHRR 45 ECtHR

Klass v Germany (1979-80) 2 EHRR 214

Malone v United Kingdom (1985) 7 EHRR 14 ECtHR

McVeigh, O'Neill and Evans v United Kingdom (1981) 5 EHRR 71

Rotaru v Romania (2000) 8 BHRC 449

Rowe and Davis v UK (2000) 30 EHRR 1

Salabiaku v France (1988) 13 EHHR 379

Von Hannover v Germany (2005) 40 EHRR 1 ECtHR

Court of Justice of the European Union Cases

Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources (C-293/12) [2014] 3 W.L.R. 1607 (ECJ (Grand Chamber))

Google Spain SL v Agencia Espanola de Proteccion de Datos (AEPD) (C-131/12) (2014) 164(7607) NLJ 20

Opinion of A.G. Cruz Villalon in *Digital Rights Ireland* (C-293/12) (2013) ECR I-845

Code of Conduct

British Society of Criminology, Code of Ethics for Researchers in the Field of Criminology, undated, 1-6 <http://www.britsoccrim.org/docs/CodeofEthics.pdf> accessed 1 February 2015

Books

Abbott, T., *Social and Personality Development* (Hove, Routledge 2001)

Abouzakhar, N., *ECCWS 2015 14th European Conference on Cyber Warfare and Security, Hatfield UK* (Reading, Academic Conferences and Publishing International Ltd 2015)

Acton, Q. A., *Issues in Law Research* (Scholarly Editions 2013)

Adams, M., Bomhoff, J., *Practice and Theory in Comparative Law* (Cambridge University Press 2012)

Adriaansens, H. P. M., *Talcott Parsons and the Conceptual Dilemma* (Abingdon, Routledge 2015)

Adshead, G., Brown, C., *Ethical Issues in Forensic Mental Health Research* (London, Kessica Kingsley Publishers Ltd 2003)

Akers, R. L., *Criminological Theories: Introduction and Evaluation* (Abingdon, Routledge 2013)

Akers, R. L., *Social Learning and Social Structure: A General Theory of Crime and Deviance* (Boston, Northeastern University Press 1998)

Akhgar, B., Brewster, B., *Combatting Cybercrime and Cyberterrorism: Challenges, Trends and Priorities* (London, Springer 2016)

Alder, J., *Constitutional and Administrative Law* (10th ed, London, Palgrave MacMillan 2015)

Alexander, J. C., *Positivism, Presuppositions, and Current Controversies* (Abingdon, Routledege 2014)

Anderson, D., *A Question Of Trust* (London, Her Majesty's Stationery Office 2015)

Anples, N. A., *Feminism and method: Ethnography, discourse analysis, and activist research* (New York, Routledge 2003)

Ary, D., Cheser Jacobs, L., Sorensen, C., Razvieh, A., *Introduction to Research in Education* (8th edn, Belmont, Wadsworth Cengage Learning 2010)

Babbie, E., *The Practice of Social Research* (14th ed, Boston, Cengage Learning 2016)

Baert, P., da Silva, F. C., *Social Theory in the Twentieth Century and Beyond* (Cambridge, Polity Press 2010)

Baggili, I., *Digital Forensics and Cybercrime: Second International ICST Conference, ICDF2C 2010, Abu Dhabi, United Arab Emirates, October 2010, Revised Selected Papers*
(London, Springer 2011)

Bainbridge, D., *Introduction to Computer Law* (5th edn, Harlow, Pearson Education Ltd 2004)

Belk, R. W., *Handbook of Qualitative Research Methods in Marketing*
(Cheltenham, Edward Elgar Publishing Ltd 2006)

Bernal, P., *Internet Privacy Rights: Rights to Protect Autonomy*
(Cambridge University Press 2014)

Blaikie, N., *Designing Social Research* (2nd ed, Cambridge, Polity Press 2010)

Blanche, M. T., Durrheim, K., Painter, D., *Research in Practice: Applied Methods for the Social Sciences (*2nd ed, Cape Town, University of Cape Town Press (Pty) Ltd 2006)

Blankenship, D. C., *Applied Research and Evaluation Methods in Recreation*
(Leeds, Human Kinetics 2010)

Blaxter, L., Hughes, C., Tight, M., *How to Research*
(3rd edn, Maidenhead, Open University Press 2006)

Bernal, P., *Internet Privacy Rights: Rights to Protect Autonomy*
(Cambridge, Cambridge University Press 2014)

Boehm, F., *Information Sharing and Data Protection in the Area of Freedom, Security and Justice, Towards Harmonised Data Protection Principles for Information Exchange at EU-level* (London, Springer 2012)

Bohm, R. M., Vogel, B., *A Primer on Crime and Delinquency Theory* (3rd ed, Belmont, Wadsworth Cengage Learning 2011)

Bohnsack, R., Pfaff, N., Weller, W., *Qualitative Analysis and Documentary Method in International Educational Research* (Barbara Budrich Publishers 2010)

Bossler, A. M., Burruss, G. W., 'The general theory of crime and computer hacking: Low self-control hackers?' in (eds) T. J. Holt, B. Schell, *Corporate hacking and technology-driven crime: Social dynamics and implications* (Hershey, IGI Global 2010) 57-81

Braun, V., Clarke, V., *Successful Qualitative Research: A Practical Guide for Beginners* (London, SAGE Publications Ltd 2013)

Brenner, S. W., *Cybercrime: Criminal Threats from Cyberspace* (Santa Barbara, Greenwood Publishing Group 2010)

Brenner, S. W., Cybercrime: Criminal Threats from Cyberspace (Santa Barbara, ABC-Clio LLC 2010)

Brink, P., 'Issues of reliability and validity' in (eds) J. Morse, *Qualitative nursing research: a contemporary dialogue* (London, SAGE 1991)

Britt, C. L., Gottfredson, M. R., *Control Theories of Crime and Delinquency*

(New Brunswick, Transaction Publishers 2003)

Bieker, F. 'The Court of Justice of the European Union, Data Retention and the Rights to Data Protection and Privacy - Where Are We Now?' in (eds) Camenisch, J., Fischer-Hübner, S., Hansen, M., *Privacy and Identity Management for the Future Internet in the Age of Globalisation* (London, Springer 2015)

Britten, N., ‘Qualitative interviews in healthcare’ in (eds) C. Pope N. Mays, *Qualitative research in health care* (2nd ed, London, BMJ Books 1999)

Brink, H., Van der Walt, C., Van Rensburg, G., *Fundamentals of Research Methodology for Health Care Professionals* (2nd ed, Cape Town, Juta & Co (Pty) Ltd 2006)

Broadhurst, R., Grabosky, P., *Cyber-Crime: The Challenge in Asia* (Hong Kong, Hong Kong University Press 2005)

Bryant, S., Bryant, R., *Policing Digital Crime* (Farnham, Ashgate Publishing Ltd 2014)

Brym, R., Lie, J., *Sociology: Your Compass for a New World*

(2nd ed, Belmont, Wadsworth Cengage 2010)

Buchanan, E. A., *Readings in Virtual Research Ethics: Issues and Controversies*

(London, Information Science Publishing 2004)

Campbell, T., *Prescriptive Legal Positivism: Law, Rights and Democracy*

(Routledge-Cavendish 2004)

Carson, D., Gilmore, S., C. Perry, C., Gronhaug, K., *Qualitative Marketing Research*

(London, SAGE Publications Inc 2005)

Casey, C., *Critical Analysis of Organizations: Theory, Practice, Revitalization*

(London, SAGE Publications Ltd 2002)

Chapman, S., *Sociology* (London, Letts and Lonsdale 2004)

Chesher, M., Kaura, R., Linton, P, Electronic Business & Commerce (London, Springer 2003)

Choo, A. L.-T., *Evidence* (3rd edn, Oxford, Oxford University Press 2012)

Church, J., Schulze, C., Strydom, H., Human Rights from a Comparative and International *Law* (University of South Africa 2007)

Claes, E., Duff, A., Gutwirth, S., *Privacy and the Criminal Law* (Oxford, Intersentia 2006)

Cookson, P. W., Sadovnik, A. R., 'Functionalist Theories of Education' in (eds) D. Levinson, P. Cookson, A. Sadovnik, *Education and Sociology: An Encyclopedia* (Abingdon, Routledge 2001)

Connaway, L. S., Powell, R. R., *Basic Research Methods for Librarians* (Santa Barbara, Greenwood Publishing Group 2010)

Conklin, W. E., *The Invisible Origins of Legal Positivism: A Re-Reading of a Tradition* (Kluwer Academic Publishers 2001)

Cooper, J, Marshall-Williams, A., *Legislating for Human Rights, The Parliamentary Debates on the Human Rights Bill* (Portland, Hart Publishing 2000)

Cotterrell, R. M., *Émile Durkheim: Law in a Moral Domain* (Stanford, Stanford University Press 1999)

Cottrell, R., McKenzie, J. F., *Health Promotion & Education Research Methods: Using the Five Chapter Thesis/Dissertation Model* (2nd ed, London, Jones and Bartlett Publishers International 2011)

Cownie, F., *Legal Academics: Culture and Identities* (Oxford, Hart Publishing 2004)

Clarke, R. V., 'Situational Prevention' in (eds) A. Von Hirsch, D. Garland, A. Wakefield, *Ethical and Social Perspectives on Situational Crime Prevention* (Oxford, Hart Publishing 2002)

Clough, J., *Principles of Cybercrime* (2nd ed, Cambridge, Cambridge University Press 2015)

Coppel, P., *Information Rights: Law and Practice* (Oxford, Hart Publishing 2014)

Creswell, J. W., Clark, V. L. P., *Designing and Conducting Mixed Methods Research*

(2nd ed, London, SAGE Publications Ltd 2011)

Cropf, R. A., Bagwell, T. C., *Ethical Issues and Citizen Rights in the Era of Digital Government Surveillance* (Hershey, Information Science Reference 2016)

Crossley, M., Arthur, L., McNess, E., *Revisiting Insider-Outsider Research in Comparative and International Education* (Oxford, Symposium Books Ltd 2015)

Cryer, P., *The Research Student's Guide to Success* (3rd edn, Maidenhead, Open University Press 2006)

Cunha, C., Manuela, M., *Handbook of Research on Digital Crime, Cyberspace Security, and Information Assurance* (Hershey, Information Science Reference 2015)

Dawson, M., Kisku, D. R., Gupta, P., Sing, J. K., Li, W., *Developing Next-Generation Countermeasures for Homeland Security Threat Prevention* (New York, IGI Global 2016)

Daymon, C., Holloway, I., *Qualitative Research Methods in Public Relations and Marketing Communications* (2nd ed, Abingdon, Routledge 2011)

de Azevedo Cunha, M. V., Market Integration Through Data Protection, An Analysis of the Insurance and Financial Industries in the EU (London, Springer 2013)

DeLisi, M., Beaver, K. M., *Criminological Theory: A Life-Course Approach* (London, Jones and Bartlett Publishers International 2011)

Dempsey, J. S., Forst, L. S., *An Introduction to Policing* (18th ed, Boston, Cengage Learning 2016)

Denscombe, M., *Ground Rules for Social Research, Guidelines for Good Practice* (2nd edn, Maidenhead, McGraw-Hill Education 2010)

Denzin, N. K., *The Research Act in Sociology* (Chicago, Aldine 1970)

DePoy, E., French Gilson, S., *The Human Experience: Description, Explanation, and Judgment* (Lanham, Rowman & Littelfield Publishing Group Inc 2007)

Dickson-Swift, V., James, E. L., Liamputtong, P., *Undertaking Sensitive Research in the Health and Social Sciences, Managing Boundaries, Emotions and Risks* (Cambridge, Cambridge University Press 2008)

Dixon, J. C., Singleton, R., Straits, B. C., *The Process of Social Research* (Oxford, Oxford University Press 2016)

Durston, G., *Evidence, Text & Materials* (2nd edn, Oxford, Oxford University Press 2011)

Easttom, C., *Computer Crime, Investigation, and the Law* (Boston, Cengage Learning 2011)

T. Edgar, 'The US Privacy Strategy' in (eds) D. Aspinall, J. Camenisch, M. Hansen, S. Fischer-Hubner, C. Raab, *Privacy and Identity Management, Time for a Revolution?* (London, Springer 2016) 20

Edmundson, W. A., *The Duty to Obey the Law: Selected Philosophical Readings* (Oxford, Rowman & Littlefield Publishers Inc, 1999)

Edwards, R., J. Holland, J., *What is Qualitative Interviewing?* (London, Bloomsbury Academic 2013)

Egbert, J., Sanden, S., *Foundations of Education Research: Understanding Theoretical Components* (Abingdon, Routledge 2014)

Emmerson, B., A. Ashworth, A., Macdonald, A., *Human Rights and Criminal Justice* (3rd ed, London, Sweet & Maxwell 2012)

Fafinski, S., *Computer Misuse: Response, Regulation and the Law* (Abingdon, Routledge 2014)

Fairholm, I., *Issues, Debates and Approaches in Psychology* (Basingstoke, Palgrave Macmillan 2012)

Faulkner, A., *The Ethics of Survivor Research: Guidelines for the Ethical Conduct of research carried out by mental health service users and survivors* (Bristol, The Policy Press 2004)

Fenwick, H., *Civil Liberties and Human Rights* (4th edn, Abingdon, Routledge-Cavendish 2007)

Fenwick, H., *Civil Liberties and Human Rights* (4th ed, Abingdon, Routledge 2009)

Fortune, A. E., Reid, W. J., Miller, R. L., *Qualitative Research in Social Work* (2nd ed, New York Columbia University Press 2013)

Foster, S., *The Judiciary, Civil Liberties and Human Rights* (Edinburgh, Edinburgh University Press 2006)

Fuchs, C., Boersma, K., Albrechtslund, A., Sandoval, M., *Internet and Surveillance: The Challenges of Web 2.0 and Social Media* (Abingdon, Routledge 2012)

Gassen, J., Gerhards-Padilla, E., Martini, P., 'Botnets: How to Fight the Ever-Growing Threat on a Technical Level' in (eds) H. Tiirmaa-Klaar, J. Gassen, E. Gerhards-Padilla, P. Martini, *Botnets* (London, Springer 2013)

Gearey, A., Morrison, W., Jago, R., *The Politics of the Common Law: Perspectives, Rights, Processes, Institutions* (2nd ed, Abingdon, Routledge 2013)

Gelman, A., Cortina, J., *A Quantitative Tour of the Social Sciences* (Cambridge, Cambridge University Press 2009)

Gibbs, G. R., *Analysing Qualitative Data* (London, SAGE Publications Ltd 2007)

Gillespie, A., *The English Legal System* (Oxford, Oxford University Press 2013)

Gillespie, A. A., *Cybercrime: Key Issues and Debates* (Abingdon, Routledge 2016)

Given, L. M., *The SAGE Encyclopedia of Qualitative Research Methods* (London, SAGE Publications Ltd 2008)

Given, L. M., *The Sage Encyclopedia of Qualitative Research Methods, Volume 2* (London, SAGE 2008)

Glover, R., Murphy, P., *Murphy on Evidence* (13th edn, Oxford, Oxford University Press 2013)

González, W. J., *New Methodological Perspectives on Observation and Experimentation in Science* (La Coruna, Netbiblo 2010)

Gooch, G., Williams, M., *A Dictionary of Law Enforcement* (Oxford, Oxford University Press 2007)

Goode, E., *Out of Control: Assessing the General Theory of Crime* (Stanford, Stanford University Press 2008)

Goold, B. J., Neyland, D., *New Directions in Surveillance and Privacy* (Cullompton, Willan Publishing 2009)

Gordley, J., Taylor von Mehren, A., *An Introduction to the Comparative Study of Private Law, Readings, Cases, Materials* (Cambridge, Cambridge University Press 2006)

Gosselin, M., *Nominalism and Contemporary Nominalism: Ontological and Epistemological Implications of the work of W.V.O. Quine and of N. Goodman* (Dordrecht, Kluwer Academic Publishers 1990)

Gottfredson, M. R., Hirsch, T., *A General Theory of Crime* (Stanford, Stanford University Press 1990)

Gottshalk, P., *Policing Cybercrime* (Ventus Publishing ApS 2010)

Gray, D. E., *Doing Research in the Real World* (3rd edn, London, Sage Publications Ltd 2014)

Greene, J. C., *Mixed Methods in Social Inquiry* (San Francisco, John Wiley & Sons Inc 2007)

Gregory, M., Glance, D., *Security and the Networked Society* (London, Springer 2013)

Gu, M., *Understanding Chinese Company Law* (2nd edn, Hong Kong University Press 2010)

Guba, E. G., Lincoln, Y. S., 'Competing paradigms in qualitative research' in (eds) N. K. Denzin, Lincoln, Y. S., *Handbook of Qualitative Research* (Thousand Oaks, SAGE 1994) 105-117

Gutwirth, S., Leenes, R., de Hert, P., Poullet, Y., *European Data Protection: Coming of Age* (Cambridge, Cambridge University Press 2014)

Guest, G., MacQueen, K. M., *Handbook for Team-based Qualitative Research* (Lanham, Altamira Press 2008)

Gutteridge, H., *Comparative law; an introduction to the comparative method of legal study and research* (2nd edn, Wildy 1974)

Gutwirth, S., Poullet, Y., De Hert, P., *Reinventing Data Protection?* (Springer 2009)

Haggerty, K. D., Ericson, R. V., 'The new politics of surveillance and visibility' in (eds) K. D. Haggerty and R. V. Ericson, *The new politics of surveillance and visibility* (Toronto, University of Toronto Press 2006)

Harding, C., Harfield, K., *Covert Investigation* (3rd edn, Oxford, Oxford University Press 2012)

Harfield, C., *Blackstone's Police Operational Handbook: Practice and Procedure* (Oxford, Oxford University Press 2009)

Hargreaves, C., Chivers, H., 'Detecting Hidden Encrypted Volumes' in (eds) De Decker, B. Schaumüller-Bichl, I., *Communications and Multimedia Security: 11th IFIP TC 6/TC 11 International Conference, CMS 2010, Linz, Austria, Ma/June 2010, Proceedings* (New York, Springer 2010)

Hartas, D., *Educational Research and Inquiry: Qualitative and Quantitative Approaches* (London, Continuum International Publishing Group 2010)

Hassard, J., *Sociology and Organization Theory: Positivism, Paradigms and Postmodernity* (Oxford, Oxford University Press 1995)

Hatch, A. J., *Doing Qualitative Research in Education Settings* (New York, State University of New York, 2002)

Hatch, J. A., *Doing Qualitative Research in Education Settings* (Albany, State University of New York Press 2002)

Hedley, S., *The Law of Electronic Commerce and the Internet in the UK and Ireland* (London, Cavendish Publishing Ltd 2006)

Heil, J., *Philosophy of Mind: A Contemporary Introduction* (London, Routledge 2002)

Hess, K. M., Orthmann, C. H., Cho, H. L., *Police Operations: Theory and Practice* (6th ed, Boston, Cenage Learning 2013)

Hesse-Biber, S. N., *Mixed Methods Research, Merging Theory with Practice* (New York, The Guildford Press 2010)

Hess Orthmann, C., Hess, K., *Criminal Investigation* (10th edn, Clifton Parl, Delmar Cengage Learning 2013)

Hill, J. B., Marion, N. E., *Introduction to Cybercrime: Computer Crimes, Laws, and Policing in the 21st Century* (Santa Barbara, ABC-CLIO LLC 2016)

Hindelang, M., Gottfredson, M., Garofalo, J., *Victims of personal crime: An empirical foundation for a theory of personal victimization* (Cambridge, Ballinger 1978)

Hirschel, D., Wakefield, W., Sasse, S., *Criminal Justice in England and the United States* (London, Jones and Bartlet Pubishers 2008)

Hirst, P. Q., *Durkheim, Bernard and Epistemology* (Abingdon, Routledge 2011)

Ho, A. T. S., *Handbook of Digital Forensics of Multimedia Data and Devices* (Chichester, John Wiley & Sons Ltd 2015)

Holloway, I., Brown, L., *Essentials of a Qualitative Doctorate* (Walnut Creek, Left Coast Press Inc 2012)

Holloway, I., *Qualitative Research in Health Care* (Maidenhead, Open University Press 2005)

Holloway, I., Wheeler, S., *Qualitative Research in Nursing and Healthcare* (3rd ed, Chichester, John Wiley & Sons 2010)

Holt, T. J., Bossler, A. M., *Cybercrime in Progress: Theory and Prevention of Technology-enabled Offenses* (Abingdon, Routledge 2016)

Holt, T. J., Bossler, A. M., Seigfried-Spellar, K. C., *Cybercrime and Digital Forensics: An Introduction* (Abingdon, Routledge 2015)

House of Lords, European Union Committee, 5th Report of Session 2013-14, Follow-up report on EU police and criminal justice measures: The UK's 2014 opt-out decision (London, TSO 2013)

House of Lords, *House of Commons, Joint Committee on Human Rights, Legislative Scrutiny: (1) Serious Crime Bill, (2) Criminal Justice and Courts Bill (second Report) and (3) Armed Forces (service Complaints and Financial Assistance) Bill, Second Report of Session 2014-15. HL Paper 49, HC 746* (London, the Stationery Office Ltd 2014)

House of Lords, House of Commons, Joint Committee on Human Rights, Legislative Scrutiny: Counter-Terrorism and Security Bill, Fifth Report of Session 2014-15 (London, The Stationery Office Ltd 2015)

Hughes, J., Sharrock, W., *Theory and Methods in Sociology: An Introduction to Sociological Thinking and Practice* (Basingstoke, Palgrave Macmillan 2007)

Hung, E., *Philosophy of Science Complete: A Text on Traditional Problems and Schools of Thought* (2nd ed, Boston, Wadsworth Cengage Learning 2014)

Hutchinson, T., *Researching and Writing in Law* (3rd edn, London, Reuters Thomson 2010)

Information Resources Management Association, *Cybercrime: Concepts, Methodologies, Tools and Applications* (Hershey, Information Science Publishing 2012)

IOS Press, *Best Practices in Computer Network Defense: Incident Detection and Response* (Geneva, IOS Press 2014)

Ismail, N., Cieh, E. L. Y., *Beyond Data Protection, Strategic Case Studies and Practical Guidance* (London, Springer 2013)

Israel, M., Hay, I., *Research Ethics for Social Scientists* (London, SAGE Publications Ltd 2006)

Israel, S. E., Lassonde, C. A., *The Ethical Educator, Integrating Ethics within the Context of Teaching and Teacher Research* (New York, Peter Lang Publishing Inc 2007)

Jain, A., *Cybercrime: Cybercrime: Issues and Threats and Management* (Delhi, Isha Books 2005)

Jaishankar, K., *Cyber Criminology: Exploring Internet Crimes and Criminal Behavior* (Boca Raton, CRC Press 2011)

Jalaalzaai, M. O., *Fixing the EU Intelligence Crisis: Intelligence Sharing, Law Enforcement and the Threat of Chemical, Biological, and Nuclear Terrorism* (New York, Algora Publishing 2016)

Jewkes, Y., Yar, M., *Handbook of Internet Crime* (Abingdon, Willan Publishing 2011)

Johnson, R., Gray, R., 'A history of philosophical and theoretical issues for mixed methods research' in (eds) A. Tashakkori, C. Teddlie, *SAGE Handbook of Mixed Methods in Social & Behavioral Research* (California, SAGE 2010) 69-94

Joint Committee on Human Rights, *Counter-Terrorism Policy and Human Rights: Terrorism Bill and related matters, Third Report of Session 2005-2006, Volume II-Oral and Written Evidence* (London, Stationery Office 2005)

Kahn, H., Jones, E., *On Thermonuclear War* (London, Transaction Publishers 2007)

Kasi, P. M., *Research: What, Why and How?: a Treatise from Researchers to Researchers* (Bloomington, Author House 2009)

Keane, A., McKeown, P., *The Modern Law of Evidence* (9th edn, Oxford University Press 2012)

Keane, A., McKeown, P., *The Modern Law of Evidence* (10th ed, Oxford, Oxford University Press 2014)

Keller, W. W., *Democracy Betrayed: The Rise of the Surveillance Security State* (Berkeley, Counterpoint 2017)

King, N., Horrocks, C., *Interviews in Qualitative Research* (London, SAGE Publications Ltd 2010)

King, N., Horrocks, C., *Interviews in Qualitative Research* (London, SAGE Publications 2010)

Kirpitchenko, L., Voloder, L., *Insider Research on Migration and Mobility: International Perspectives on Researcher Positioning* (Farnham, Ashgate Publishing Ltd 2014)

Kirwan, G., *The Psychology of Cybercrime: Concepts and Principles: Concepts and Principles* (Hershey, Information Science Reference 2012)

Klimek, L., *European Arrest Warrant* (London, Springer 2015)

Klitou, D., *Privacy-Invading Technologies and Privacy by Design: Safeguarding Privacy, Liberty and Security in the 21st Century* (The Hague, TMC Asser Press 2014)

Knight, A., Ruddock, L., *Advanced Research Methods in the Built Environment* (Chichester, Blackwell Publishing Ltd 2008)

Kshetri, N., *The Global Cybercrime Industry: Economic, Institutional and Strategic Perspectives* (London, Springer-Verlag 2010)

Kshetri, N., *The Global Cybercrime Industry: Economic, Institutional and Strategic Perspectives* (London, Springer 2010)

Kuada, J., *Research Methodology: A Project Guide for University Students* (Frederiksberg, Samfundslitteratur 2012)

Langer, L., *Religious Offence and Human Rights: The Implications of Defamation of Religions* (Cambridge, Cambridge University Press 2014)

Leavy, P., *The Oxford Handbook of Qualitative Research* (Oxford, Oxford University Press 2014)

Lee, R. M., *Doing Research on Sensitive Topics* (London, SAGE 1993)

Lehmann Imfeld, Z., Hampson, P., Milbank, A., *Theology and Literature after Postmodernity* (London, Bloomsbury T & T Clark 2015)

Lindenfeld, D. F., *The Transformation of Positivism: Alexius Meinong and European Thought, 1880-1920* (Los Angeles, University of California Press 1980)

Littlejohn Shinder, D., Cross, M., *Scene of the Cybercrime* (Burlington, Syngress Publishing Inc 2008)

Lloyd, I. J., Cyber Law in the United Kingdom (AH Alphne aan den Rijn, Kluwer Law International 2010)

Lloyd, I. J., *Information Technology Law* (6th edn, Oxford, Oxford University Press 2011)

LoBiondo-Wood, G., Haber, J., *Nursing Research: Methods, Critical Appraisal and Utilisation* (2nd ed, St Louis, Mosby 1998)

Long, T., Johnson, M., *Research Ethics in the Real World: Issues and Solutions for Health and Social Care* (Philadelphia, Elsevier Ltd 2007)

MacCormick, N., Weinberger, O., *An Institutional Theory of Law: New Approaches to Legal Positivism* (Springer 1986)

MacKinnon, R., Hickok, E., A. Bar, H-I. Lim, *Fostering freedom online: the role of Internet intermediaries* (Paris, UNESCO 2015)

Manoharan, A., Holzer, M., *Active Citizen Participation in E-Government: A Global Perspective* (Hershey, Information Science Reference 2012)

Marcovici, M., *The Surveillance Society: The security vs. privacy debate* (Norderstedt, Books on Demand 2013)

Martin, C. R., Weakley, S. L., *Internet Law and Practice in California* (Oakland, CEB 2015)

Martin, G., Scott Bray, R., Kumar, M., *Secrecy, Law and Society* (Abingdon, Routledge 2015)

Mason, J., *Qualitative Researching* (London, SAGE 1996)

Matheson, J., 'Epistemic Relativism' in (eds) A. Cullison, *The Bloomsbury Companion to Epistemology* (London, Bloomsbury 2014) Chapter 9

Mayhew, P., Clarke, R. V., Hough, M., Sturman, A., *Crime as Opportunity*, Home Office Research Study No.34 (London, HMSO 1973)

McConville, M., Hong Chui, W., *Research Methods for Law* (Edinburgh University Press 2007)

McClean, J. D., *International Co-operation in Civil and Criminal Matters* (Oxford, Oxford University Press 2002)

McLeod, J., Hare, C., *How to Manage Records in the e-Environment* (Abingdon, Routledge, 2010)

McNabb, D. E., *Research Methods in Public Administration and Nonprofit Management, Quantitative and Qualitative Approaches* (New York, M. E. Sharpe Inc 2013)

McShane, M., Williams, F. P., *Victims of Crime and the Victimization Process* (Abingdon, Routledge 2013)

Mendel, T., Puddephatt, A., Wagner, B., Hawtin, D., Torres, N., *Global Survey on Internet Privacy and Freedom of Expression* (Paris, United Nations Educational, Scientific and Cultural Organization 2012)

Merton, R. K., *Social Theory and Social Structure* (New York, The Free Press 1948)

Merriam, S. B., *Qualitative Research: A Guide to Design and Implementation* (San Francisco, John Wiley & Sons 2009)

Merriam, S. B., Tisdell, E. J., *Qualitative Research: A Guide to Design and Implementation* (San Francisco, John Wiley & Sons 2016)

Merrin, W., *Media Studies 2.0* (Abingdon, Routledge 2014)

Michalski, R. L., Shackelford, T. K., 'Evolutionary Perspectives on Personality Psychology' in (eds) G. J. Boyle, G. Matthews, D. H. Saklofsk, *The SAGE Handbook of*

Personality Theory and Assessment, Vol.2 Personality Measurement and Testing (London, SAGE 2008)

Miller, J. M., *The Encyclopedia of Theoretical Criminology* (London, Wiley Blackwell 2014)

Miller, R., Cross, F., *The Legal Environment Today: Business In Its Ethical, Regulatory, E-Commerce, and Global Setting* (7th edn, Mason, South-Western Cengage Learning 2013)

Mitchell, M., Jolley, J., *Research Design Explained* (7th ed, Belmont, Wadsworth 2010)

Monateri, P. G., *Methods of Comparative Law* (Edward Elgar Publishing Ltd 2012)

Morrow, R. A., Torres, C. A., *Social Theory and Education: A Critique of Theories of Social and Cultural Reproduction* (Albany, State University of New York 1995)

Morse, J. M., 'Strategies for sampling' in (eds) J. M. Morse, Qualitative Nursing Research: A Contemporary Dialogue (Newsbury Park, SAGE 1991)

Munday, R., *Evidence* (7th edn, Oxford, Oxford University Press 2013)

Nagyfejeo, E., 'Transatlantic collaboration in countering cyberterrorism' in (eds) L. Jarvis, S. Macdonald, T. M. Chen, *Terrorism Online: Politics, Law and Technology* (Abingdon, Routledge 2015)

Newburn, T., Neyroud, P., *Dictionary of Policing* (Willan Publishing 2013)

Nicholls, C., Montgomery, C., Knowles, |J. B., Doobay, A., Summers, M., *Nicholls, Montgomery, and Knowles on The Law of Extradition and Mutual* (3rd ed, Oxford, Oxford University Press 2013)

OECD, *Global Forum on Transparency and Exchange of Information for Tax Purposes, Peer Review Report Phase 1, Legal and Regulatory Framework United Arab Emirates* (Paris, OECD 2012)

Oleksy, M. W., *Realism and Individualism: Charles S. Peirce and the Threat of Modern Nominalism* (Amsterdam, John Benjamins Publishing Co 2015)

Orakhelashvili, A., *Research Handbook on Jurisdiction and Immunities in International Law* (Cheltenham, Edward Elgar Publishing Ltd 2015)

Ormerod, D., *Blackstone's Criminal Practice 2012* (Oxford, Oxford University Press 2011)

Osterburg, J. W., Ward, R. H., Criminal Investigation: A Method for Reconstructing the Past (7th ed, Abingdon, Routledge 2014)

Oxford Business Group, *The Report: Abu Dhabi 2010* (Oxford, Oxford Business Group 2010)

Parsons, T., *The Structure of Social Action* (London, McGraw Hill 1937)

Park, R. E., Burgess, E. W., McKenzie, R. D., *The city*
(Chicago, The University of Chicago Press 1925)

Patton, M. W., *Qualitative Research & Evaluation Methods: Integrating Theory and Practice* (4th ed, London, SAGE Publications Ltd 2015)

Perry, W. L., McInnis, B., Price, C. C., Smith, S. C., Hollywood, J. S., *Predictive Policing: The Role of Crime Forecasting in Law Enforcement Operations*
(New York, RAND Corporation 2013)

Petre, M., Rugg, G., *The Unwritten Rules of PhD Research* (2nd edn, Maidenhead, Open University Press 2010)

Pitney, W. A., Parker, J., *Qualitative Research in Physical Activity and the Health Professions* (Leeds, Human Kinetics 2009)

Pivcevic, E., *Husserl and Phenomenology* (Routledge 2014)

Polit, D., Hungler, B., *Nursing research: Principles and methods* (New York, JB Lippincott 1991)

Prasad, S. K., Routray, S., Khurana, R., *Information Systems, Technology and Management* (Berlin, Springer-Verlag 2009)

Prins, J. E. J., Ribbers, P. M. A., *Trust in Electronic Commerce: The Role of Trust from a Legal, an Organizational and a Technical Point of View* (Kluwer Law International 2002)

Quimby, E., *Doing Qualitative Community Research: Lessons for Faculty, Students and Communities* (Danvers, Bentham Science Publishers 2012)

Ramraj, V. V., Hor, M., Roach, K., *Global Anti-Terrorism Law and Policy* (Cambridge, Cambridge University Press 2005)

Redpath, S. M., Gutiérrez, R. J., A Evely, A., Wood, K. A., Young, J. C., *Conflicts in Conservation* (Cambridge, Cambridge University Press 2015)

Reiner, R., *The Oxford Handbook of Criminology* (4th ed, Oxford, Oxford University Press 2007)

Reuvid, J., *The Secure Online Business Handbook: A Practical Guide to Risk Management and Business Continuity* (4th edn, London, Kogan Page Ltd 2006)

Richardson, M., Bryan, M., Vranken, M., Barnett, K., *Breach of Confidence, Social Origins and Modern Developments* (Cheltenham, Edward Elgar Publishing Ltd 2012)

Ridenour, C. S., Newman, I., *Mixed Methods Research, Exploring the Interactive Continuum* (Southern Illinois University 2008)

Ritzer, G., Ryan, J. M., *The Concise Encyclopedia of Sociology* (Chichester, John Wiley & Sons 2011)

Rogers, C., Lewis, R., John, T., Read, T., *Police Work: Principles and Practice* (Abingdon, Routledge 2011)

Ross, H., *Law as a Social Institution* (Portland, Hart Publishing 2001)

Russell, C., Hogan, L., Junker-Kenny, M., *Ethics for Graduate Researchers, A Cross-Disciplinary Approach* (London, Elsevier Inc 2013)

Saini, M., Shlonsky, A., *Systematic Synthesis of Qualitative Research* (Oxford, Oxford University Press 2012)

Sammens, J. Rajewski, J., *The Basics of Digital Forensics: The Primer For Getting in Digital Forensics* (Elsevier Inc 2012)

Sandelowski, M., Barroso, J., *Handbook for Synthesizing Qualitative Research* (New York, Springer Publishing Company Inc 2007)

Savin, A., Trzaskowski, J., *Research Handbook on EU Internet Law* (Cheltenham, Edward Elgar Publishing Limited 2014)

Savona, E. U., *Crime and Technology: New Frontiers for Regulation, Law Enforcement and Research* (Dordrecht, Springer 2004)

Scaife, L., *Handbook of Social Media and the Law* (Abingdon, Routledge 2015)

Schatzman, L., Strauss, A. L., *Field Research Strategies for a Natural Sociology* (Englewood Cliffs, Prentice Hall 1973)

Schjolberg, S., *The History of Cybercrime: 1976-2014* (Norderstedt, Cybercrime Research Institute GmbH 2014)

Scott, D., Morrison, M., *Key Ideas in Educational Research* (London, Continuum International Publishing Group 2006)

Secretary of State for the Home Department, *Draft Communications Data Bill, Cm 8359* (London, TSO Shop Ltd 2012)

Seidel, M., *Epistemic Relativism: A Constructive Critique* (Basingstole, Palgrave Macillan 2014)

Shaw, C. R., McKay, H. D., *Juvenile Delinquency in Urban Areas* (Chicago, University of Chicago Press 1942)

Sieber, J., *Planning ethically responsible research: A guide for students and internal review boards* (Newbury Park Sage 1992)

Siegel, L. J., *Criminology* (11th ed, Belmont, Wadsworth Cengage Learning 2012)

Silverman, D., *Doing Qualitative Research: A Practical Handbook* (4th ed, London, SAGE Publications Ltd 2013)

Silverman, D., *Interpreting qualitative data: Methods for analysing talk, text and interaction* (2nd ed, London, Sage Publications 2001)

Sinn, R., *Software Security Technologies, A Programmatic Approach* (Stamford, Cengage Learning 2008)

Siltala, R., *A Theory of Precedent: From Analytical Positivism to a Post-analytical Positivism to a Post-analytical Philosophy of Law* (Oxford, Hart Publishing 2000)

Sirohi, M. N., *Transformational Dimensions of Cybercrime* (Delhi, Alpha Editions 2015)

Smartt, U., *Media & Entertainment Law* (2nd edn, Abingdon, Routledge 2014)

Smith, R. G., Grabosky, P., Urbas, G., *Cyber Criminals on Trial* (Cambridge, Cambridge University Press 2004)

Smith, G. J. J., Bird & Bird, *Internet Law and Regulation* (4th edn, London, Sweet & Maxwell 2007)

Smith, M. E., *Europe's Foreign and Security Policy: The Institutionalization of Cooperation* (Cambridge, Cambridge University Press 2004)

Smith, M. J., Social Science in Question London (London, Sage 1998)

Smits, J. M., *Elgar Encyclopedia of Comparative Law* (Edward Elgar Publishing Inc 2006)

Snooks, G., *The Laws of History* (Abingdon, Routledge 1998)

Stahl, B. C., *Information Systems, Critical perspectives* (Abingdon, Routledge 2008)

Stalla-Bourdillon, S., Phillips, J., Ryan, M. D., *Privacy vs. Security* (London, Springer 2014)

Standing, C., *How to Complete a PhD* (Craig Standing 2012)

Stevenson, A., *Oxford Dictionary of English* (Oxford, Oxford University Press 2010)

Subramanian, R., *Computer Security, Privacy, and Politics: Current Issues, Challenge, and Solutions* (IRM Press 2008)

Summers, S., Schwarzenegger, C., Ege, G., Young, F., *The Emergence of EU Criminal Law: Cybercrime and the Regulation of the Information Society* (Oxford, Hart Publishing 2014)

Tapper, C., *Cross & Tapper on Evidence* (12th edn, Oxford, Oxford University Press 2010)

Thomas, D., Loader, B., *Cybercrime: Law Enforcement, Security and Surveillance in the Information Age* (London, Routledge 2000)

Thomas, D., Loader B. D., 'Cybercrime: law enforcement, security and surveillance in the information age' in (eds) B. D. Loader, D. Thomas, *Cybercrime: Security and Surveillance in the Information Age* (Abingdon, Routledge 2005)

Tibbetts, S. G., Hemmens, C., *Criminological Theory: A Text/Reader* (London, SAGE 2010)

Tonry, M. H., *The Handbook of Crime & Punishment* (Oxford, Oxford University Press 1998)

Torremans, P., *Research Handbook on Cross-border Enforcement of Intellectual Property* (Cheltenham, Edward Elgar Publishing Ltd 2014)

Trainor, A. A., Graue, E., *Reviewing Qualitative Research in the Social Sciences* (Routledge 2013)

Tsagourias, T., Buchan, R., *Research Handbook on International Law and Cyberspace* (Cheltenham, Edward Elgar Publishing Limited 2015)

Turner, M., Pantlin, N., Pugh, L., Young, C., EU Cybercrime Directive takes a tougher stance against attacks on information systems, Herbert Smith Freehills LLP, 2013 <http://www.lexology.com/library/detail.aspx?g=d3863b21-3c3b-419e-8a8f-2b007acb3a10> accessed 1 July 2014

Twining, W., *General Jurisprudence, Understanding Law from a Global Perspective* (Cambridge University Press 2009)

United Kingdom House of Commons: Science and Technology Committee, *Malware and cybercrime: Twelfth Report of Session 2010-12, HC 1537* (London, TSO Shop 2012)

United Nations Conference on Trade and Development, *Information Economy Report 2005* (New York, United Nations 2005)

US National Intelligence Council, *Global Trends 2030: Alternative Worlds* (Washington DC, US Government Printing Office 2012)

Von Bar, C., *Non-Contractual Liability Arising out of Damage Cause to Another* (Munich, European Law Publishers 2009)

Van Hoecke, M., *Preference to Methodologies of Legal research, which kind of method for What Kind of Discipline?* (London, Hart Publishing 2011)

Van Orman Quine, W., Føllesdal, D., Quin, D. B., *Confessions of a Confirmed Extensionalist: And Other Essays* (Harvard, Harvard University Press 2008)

Vito, G. F., Maahs, J. R., Holmes, R. M., C*riminology: Theory, Research, and Policy* (2nd ed, London, Jones and Bartlett Publishers 2007)

Walker, C., *Terrorism and the Law* (Oxford, Oxford University Press 2011)

Wall, D.,, *Cybercrime: The Transformation of Crime in the Information Age,* (Polity Press, 2007)

Walters, G. D., *Criminal Belief Systems: An Integrated-Interactive Theory of Lifestyles: An Integrated-Interactive Theory of Lifestyles* (Westport, Praeger Publishers 2002)

Watkins, D., Burton, M., *Research Methods in Law* (Routledge 2013)

Wearne, B. C., *The Theory and Scholarship of Talcott Parsons to 1951: A Critical Commentary* (Cambridge, Cambridge University Press 2009)

Westby, J., *International Guide to Combating Cybercrime* (Chicago, ABA Publishing 2003)

Wiles, R., *What are Qualitative Research Ethics?* (London, Bloomsbury Academic 2013)

Williams, I. R., *Strategic Planning in Small Businesses: A phenomenological study investigating the role, challenges, and best practices of strategic planning* (Minnesota, ProQuest 2008)

Willis, J., *Qualitative Research Methods in Education and Educational Technology* (Charlotte, Information Age Publishing Inc 2008)

Wong, R., *Data Security Breaches and Privacy in Europe* (London, Springer 2013)

Yates, S. J., *Doing Social Science Research* (London, SAGE 2003)

Yin, R. K., *Case Study Research: Design and Methods* (4th edn, Sage Publications 2009)

Yin, R. K., *Qualitative Research from Start to Finish*
(2nd ed, New York, The Guilford Press 2016)

Zagaris, B., *International White Collar Crime: Cases and Materials* (2nd ed, Cambridge, Cambridge University Press 2015)

Zweiaert, K., Koetz, H., *An Introduction to Comparative Law* (Oxford University Ores 1998)

Journal Articles

-- (2018) ‘Legislative Comment: Data Protection Bill 2017’, Immigration, Asylum and Nationality Law 32(2) 98-99

Agate, J., Ledward, J., Social media: how the net is closing in on cyber bullies, 24(8) *Entertainment Law Review* 2013, 263-268

Akdeniz, Y., Taylor, N., Walker, C., 'Regulation of Investigatory Powers Act 2000 (1): Bigbrother.gov.uk: State surveillance in the age of information and rights' (2001) *Criminal Law Review*, 73-90

Akdeniz, Y., Taylor, N., Walker, C., Bigbrother.gov.uk: state surveillance in the age of information and rights, *Criminal Law Review* 2001, 73-90

Akers, R. L., Lee, G., A longitudinal test of social learning theory: Adolescent smoking, 26 *Journal of Drug Issues* 1996, 317-343

Akhtar, Z., Malicious communications, media platforms and legal sanctions, 20(6) *Computer and Telecommunications Law Review* 2014, 179-187

Aljneibi, K. A., The Regulation of Electronic Evidence in the United Arab Emirates: Current Limitations and Proposals for Reform, PhD Thesis, February 2014, 1-326 <http://e.bangor.ac.uk/4992/1/Aljneibi%20khaled%20thesis.pdf> accessed 15th February 2017

Al-Khouri, A. M., 'e-Government Strategies, The Case of the United Arab Emirates' (2012) 17 *European Journal of e-Practice*, 126-150

Al Neaimi, A., 'A Critical Analysis of the Effectiveness of Cyber Security Defenses in UAE Government Agencies' (2014) *Proceedings of the International Conference on Information Security and Cyber Forensics*, Kuala Terengganu, Malaysia, 36-43

Al Neyadi, A., Al Kaabi, A., al Kabi, L., Al Ghufli, M., Al Sahmsi, M. Khan, M., 'Internet Governance & Cybercrimes in UAE (2015) 4(11) *International Journal of Scientific & Technology Research*, 350-357

Aloul, F., Information security awareness in UAE: A Survey paper (2010) Internet Technology and Secured Transactions, 1-6

Baez, B., Confidentiality in qualitative research: Reflections on secrets, power and agency, 2 *Qualitative Research* 2002, 35–58

Balz, K., Almousa, A. S., The Recognition and Enforcement of Foreign Judgements and Arbitral Awards under the Riyadh Convention 1983, Third Years of Arab Judicial Co-operation, 4(2) *International Journal of Procedural Law* 2014, 273-288

Basamh, S. S., Qudaih, H. A., Bin Ibrahim, J., 'An overview on Cyber Security Awareness in Muslim Countries' (2014) *International Journal of Information and Communication Technology*, 21-24

Battcock, R., 'Prosecutions under the Computer Misuse Act' (1996) *Computers and Law,* 6

Beheshti, P., Keeping IT safe (2016) *Emirates Law Business & Practice*, 5-7

Beheshti, B., Hambly, V., 'To Post...or Not to Post?' (2016) *Emirates Law Business & Practice*, 23-24

Bergman, M. M., Coxon, A. P. M., The Quality in Qualitative Methods, 6(2) *Qualitative Social Research* 2005, 34 <http://www.qualitative-research.net/index.php/fqs/article/view/457/974#g21> accessed 15th July 2015

Blevins, K. R., Holt, T. J., Examining the virtual subculture of johns, 38(5) *Journal of Contemporary Ethnography* 2009, 619-648#

Boeringer, S., Shehan, C. L., Akers, R. L., Social contexts and sexual learning in sexual coercion and aggression: Assessing the contribution of fraternity membership, 40 *Family Relations* 1991, 558-564

Bossler, A. M., THolt, T. J., May, D. C., Predicting online harassment victimization among a juvenile population, 44(4) *Youth & Society* 2012, 500-523

Bossler, A. M., Hold, T. J., The effect of self-control on victimization in the cyberworld, 38(3) *Journal of Criminal Justice* 2010, 227-236

Brannan, J., Crime and social networking sites, 1 *Juridical Review* 2013, 41-51

Brazeley, P., Teaching mixed methods, 3 *Qualitative Research Journal* 2003, 117-126

Buzzel, T., D. Foss, D., Middleton, Z. Explaining use of online pornography: A test of self-control theory and opportunities for deviance, 13 *Journal of Criminal Justice and Popular Culture* 2006, 96-116

Cameron, R., Mixed Methods Research: The Five Ps Framework, 9(2) *Electronic Journal of Business Research Methods* 2011, 96-108 <http://ejbrm.com/volume9/issue2> accessed 1st August 2015

Cannataci, J. A., Defying the logic, forgetting the facts: the new European proposal for data protection in the police sector, 4(2) *European Journal of Law and Technology* 2013 <http://ejlt.org/article/view/284/390> accessed 1 July 2014

Carr, I., Williams, K. S., Cyber-crime and the Council of Europe: reflections on a Draft Convention, 7(4) *International Trade Law & Regulation* 2001, 93-96

Case Comment, Data retention Directive invalid, says ECJ, 319 *EU Focus* 2014, 14-16

Case Comment, Data Retention Directive is declared invalid by ECJ, 19(2) *Communications Law* 2014, 38

Case Comment, Europe and US divide once again over cyber security, 13(4) *Privacy & Data Protection* 2013, 1, 17

Case Comment, Uncertainty for EU ISPs as court declares retention law invalid, 14(5) *Privacy & Data Protection* 2014, 1, 17

Case Comment, Unlawful directed surveillance, 15(4) *Communications Law* 2010, 122-123

Casilli, A. A., Four These on Digital Mass Surveillance and the Negotiation of Privacy, 8th Annual Privacy Law Scholar Congress 2015, Jun 2015, Berkeley, United States,

2015, 1-14 <https://halshs.archives-ouvertes.fr/halshs-01147832/document> accessed 1st December 2015

Cassim, F., Formulating Specialised Legislation to Address the Growing Spectre of Cybercrime: A Comparative Study, 12(4) *PER* 2009, 1-360

Charlesworth, A., 'Addiction and hacking' (1993) 143 *New Law Journal* 540

Chynoweth, P. 'Legal research', *Advanced Research Methods in the Built Environment* (Oxford, Wiley-Blackwell, 2008) 28-38

Clifford Chance, The right to privacy online in the UAE - To post or not to post? Briefing Note, February 2016, 1-3

Cohen, L., Felson, M., Social Change and Crime Rate Trends: A Routine Activity Approach, 44(4) *American Sociological Review* 1979, 588–608

Colangelo, A. J., What is extraterritorial jurisdiction? 99 *Cornell Law Review* 2014, 1303-1352

Coleman, S., E-mail, terrorism, and the right to privacy, 8 *Ethics and Information Technology* 2006, 17-27

Connect Arab Summit, Building trust and security in the use of ICTs, Background paper, 15 February 2012, 1-8

Coyne, I. T., Samplying in qualitative research. Purposeful and theoretical sampling; merging or clear boundaries? 26 *Journal of Advanced Nursing* 1997, 623-630

Clarke, R. V. G., Situational Crime Prevention: Theory and practice, 20(2) *British Journal of Criminology* 1980, 136-147

Clarvarion, A. M., Najman, J. M., Silverman, D., The Quality of Qualitative Data: Two Strategies for Analyzing Medical Interviews, 1(2) *Qualitative Inquiry* 1995, 223-242

CTOlabs.com, 'White Paper: Big Data Solutions For Law Enforcement', June 2012, 1-8 <https://theartofservicelab.s3.amazonaws.com/All%20Toolkits/The%20Big%20Data%20Solutions%20Toolkit/Act%20-%20Recommended%20Reading/Big%20Data%20Solutions%20For%20Law%20Enforcement.pdf> accessed 1st September 2017

Decker, S. E., Naugle, A. E., Carter-Visscher , R., Bell, K., Seifert, A., Ethical Issues in Research on Sensitive Topics: Participants' Experiences of Distress and Benefit, 6(3) *Journal of Empirical Research on Human Research Ethics: An International Journal* 2011, 55-64

Denscombe, M., Communities of practice: a research paradigm for the Mixed Methods approach, De Montford University, 2008, 1-26

Dickson-Swift, V., James, E. L., Kippen, S., Liamputtong, P., Risk to Researchers in Qualitative Research on Sensitive Topics: Issues and Strategies, 18(1) *Health Policy & Services* 2008, 133-144

Editorial, Admissibility; Criminal evidence; Privacy; Surveillance; Telecommunications, *Criminal Law Review* 2000, 877-878

El Guindy, M. N., Cybercrime challenges in the Middle East, 2012, Cyber Security, 1-6

ENISA, The Directive on attacks against information systems, A Good Practice Collection for the implementation and application of this Directive 2013, 1-23 <http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/Octopus2013/Presentations/Workshop1/Jo_De_Muynck-ENISA-Octopus.pdf> accessed 1 July 2014

EU Focus 2010, Commission proposes boosting Europe's defences against cyber-attacks, 277, 22-23

Evans, J. M., 'Civil Litigation - Discovery - Public Interest Immunity and State Papers' (1980) 58(2) *Canadian Bar Review* 360-376

Fafinski, S., (2006) 'Access Denied: Computer Misuse in an Era of Technological Change' 70 JCL 424

Fafinski, S., (2008) 'Computer misuse: the implications of the Police and Justice Act 2006' Journal of Criminal Law 72(1), 53-66

Falconer, D. J., Mackay, D. R., The Key to the Mixed Method Dilemma, *Proclamation of 10th Australasian Conference on Information Systems* 1999, 286-297 <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.5.148&rep=rep1&type=pdf > accessed 1st August 2015

Fahie, D., Doing Sensitive Research Sensitively: Ethical and Methodological Issues in Researching Workplace Bullying, 13(1) *International Journal of Qualitative Methods* 2014, 19-36

Feilzer, M. Y., Doing Mixed Methods Research Pragmatically: Implications for the Rediscovery of Pragmatism as a Research Paradigm, 4(1) *Journal of Mixed Methods Research* 2010, 1-16

Forsyth, C., 'Public Interest Immunity: Recent and Future Developments' (1997) 1 *Cambridge Law Journal*, 51-59, 51

Funta, R., EU-USA Privacy Protection Legislation and the Swift Bank Data Transfer Regulation: A Short Look, 5(1) *Masaryk University Journal of Law and Technology* 2011, 23-33

Fusch, P. I., Ness, L. R., Are We There Yet? Data Saturation in Qualitative Research, 9(1) *The Qualitative Report* 2015, 1408-1416

Garratt, D., Hodkinson, P., Can there be criteria for selecting research criteria? - A hermeneutical analysis of an inescapable dilemma, 4(3) *Qualitative Inquiry* 1998, 515-539

Gersch, A., Covert surveillance - a snoopers' charter? *Archbold Review* 2012, 5-8

Giddens, A., Classical Social Theory and the Origins of Modern Sociology, 81(4) *American Journal of Sociology* 1976, 703-729

Giddings, L. S., Grant, B. M., A Trojan Horse for Positivism?: A Critique of Mixed Methods Research, 30(1) *Advances in Nursing Science* 2007, 52-60

Gill, P., Stewart, K., Treasure, E., Chadwick, B., Methods of data collection in qualitative research: interviews and focus groups, 204 *British Dental Journal* 2008, 291-295 <http://www.nature.com/bdj/journal/v204/n6/full/bdj.2008.192.html> accessed 4th August 2015

Gillespie, A. A., Regulation of internet surveillance, 4 *European Human Rights Law Review* 2009, 552-565

Goldsmith, J., How cyber changes the laws of war, 24(1) *European Journal of International Law* 2013, 129-138

Goold, B., Liberty and others v The United Kingdom: a new chance for another missed opportunity, *Public Law* 2009, 5-14

Grady, M., Parisi, F., Walden, I., The Law and Economics of Cybersecurity, Publication Review, 13(2) *Computer and Telecommunications Law Review* 2007, 78-79

Granger, M.-P., Irion, K., The Court of Justice and the Data Retention Directive in Digital Rights Ireland: telling off the EU legislator and teaching a lesson in privacy and data protection, 39(6) *European Law Review* 2014, 835-850

Greene, M. J., On the Inside Looking In: Methodological Insights and Challenges in Conducting Qualitative Insider Research, *The Qualitative Report* 19(29), 1-13

Guest, G., Bunce, A., Johnson, L., How Many Interviews Are Enough?: An Experiment with Data Saturation and Variability, 18 *Field Methods* 2006, 59-82

Hale, A., Edwards, J., Getting it taped, 12(3) *Computer and Telecommunications Law Review* 2006, 71-73

Higgins, G. E., Can low self-control help with the understanding of the software piracy problem? 26 *Deviant Behavior* 2006, 2005, 1-24

Higgins, G. E., Wolfe, S. E., Marcum, C. D., Digital piracy: An examination of three measurements of self-control, 29 *Deviant Behavior* 2008, 440-460

Hinduja, S., Patchin, J. W., Cyberbullying: An exploratory analysis of factors related to offending and victimization, 29 *Deviant Behavior* 2008, 129-156

Hjorland, B., Empiricism, rationalism and positivism in library and information science, 61(1) *Journal of Documentation* 61(1) 2005, 130-155

Holt, T. J., Bossler, A. M., An Assessment of the Current State of Cybercrime Scholarship, 35(1) *Deviant Behavior* 2014, 20-40

Holt, T. J., Bossler, A. M., Examining the Applicability of Lifestyle-Routine Activities Theory for Cybercrime Victimization, 30(1) *Deviant Behavior* 2008, 1-25

Holt, T. J., Bossler, A. M., May, D. C., Low self-control, deviant peer associations, and juvenile cyberdeviance, 37(3) *American Journal of Criminal Justice* 2012, 378-395

Holt, T. J., Burruss, G. W., Bossler, A. M., Social learning and cyber deviance: Examining the importance of a full social learning model in the virtual world, 33(2) *Journal of Crime and Justice* 2010, 31-61

Holt, T. J., Strumsky, D., Smirnova, O., Kilger, M., Examining the social networks of malware writers and hackers, 6(1) *International Journal of Cyber Criminology* 2012, 891-903

Huey, L., Rosenberg, R. S., Watching the Web: Thoughts on Expanding Police Surveillance Opportunities under the Cyber-Crime Convention, *Canadian Journal of Criminology and Criminal Justice* 2004, 597-606

Ienco, M., Digital identity as a key enabler for e-government services, Mobile Connect, 2016, 1-8 <https://www.gsma.com/identity/wp-content/uploads/2016/02/MWCB16-Digital-Identity-as-a-Key-Enabler-for-eGovernment-Services-Marta-Ienco.pdf> accessed 1st September 2017

Jarvie, N., Control of cybercrime - is an end to our privacy on the Internet a price worth paying? Part 1, 9(3) *Computer and Telecommunications Law Review* 2003, 76-81

Jarvie, N., Control of cybercrime - is an end to our privacy on the Internet a price worth paying? Part 2, 9(4) *Computer and Telecommunications Law Review* 2003, 110-115

Jerome, O. U., Russia and the Council of Europe Convention on Cybercrime, 18(1) *Computer and Telecommunications Law Review* 2012, 16-17

Jick, T. D., 'Mixing Qualitative and Quantitative Methods: Triangulation in Action' (1979) 24 (4) *Qualitative Methodology* 602-611

Jimeno Bulnes, M., European Judicial Cooperation in Criminal Matters, 5 *European Law Journal* 2003, 614-630

Joh, E. E., 'Policing by Numbers: Big Data and the Fourth Amendment' (2014) *Washington Law Review* 89, 35-68

Johnson, R. B., Mixed Methods Research: A Research Paradigm Whose Time Has Come, 33(7) *Educational Researcher* 2004, 14-26

Jones, G. "Restitution of Benefits Obtained in Breach of Another's Confidence' (1970) 86 LQR 463

Judge Stein Schjolberg, A presentation at the Europol-INTERPOL Cybercrime Conference, Europol, The Hague, 24-25 September 2013, 1-15 <http://www.cybercrimelaw.net/documents/Europol-INTERPOL.pdf> accessed 15th February 2017

Kalekin-Fishman, D., Review: David Silverman (2001). 'Interpreting qualitative data: Methods for analysing talk, text and interaction' (2001) 2(3) *Forum Qualitative Social Research*, 1

Khan, C., Caught in the net, *The Brief*, November 2009, 23-24

Keenan, B., Bulk data in the draft Investigatory Powers Bill: the challenge of effective oversight, LSE Law Policy Briefing Series 13, 2015, 1-4 <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2703839> accessed 1st December 2015

Kelly, J. X., Computer Misuse Overview, JISC Legal Information, 2007 <http://www.jisclegal.ac.uk/LegalAreas/ComputerMisuse/ComputerMisuseOverview.aspx> accessed 17 June 2014

Konstadinides, T., Destroying democracy on the ground of defending it? The Data Retention Directive, the surveillance state and our constitutional ecosystem, 36(5) *European Law Review* 2011, 722-736

Kozlovski, N., A Paradigm Shift in Online Policing - Designing Accountable Policing, Yale Law School, 2005, 1-22 <https://crypto.stanford.edu/portia/papers/Kozlovski.pdf> accessed 1st March 2017

Kuhling, J., Heitzer, S., Returning through the National Back Door? The future of data retention after the ECJ Judgment on Directive 2006/24 in the UK and Elsewhere, 2 *European Law Review* 2015, 263-278

Kuper, A., Critically appraising qualitative research, 33(7) *British Medical Journal* 2008 <http://www.bmj.com/content/337/bmj.a1035.full?ijkey=21e4db22678d417636de04f2b64921e4a58ffff0&keytype2=tf_ipsecsha> accessed 1st August 2015

Kaiser, K., Protecting Respondent Confidentiality in Qualitative Research, 19(11) *Qualitative Health Research* 2009, 1632-1641

Kwangjo, K., Kaist, D., Challenges of Cyber Security for Nuclear Power Plants, Khalifa University of Science, Technology and Research, Abu Dhabi, UAE, 18th Pacific Basin Nuclear Conference, BEXCO, Busan, Korea, 2012, 1-7 <http://caislab.kaist.ac.kr/publication/paper_files/2012/PBNC2012-kkj.pdf> accessed 20th April 2016

Lestrade, E., The cybercrime phenomenon and Latvian cybercrime law, *European Newsletter* 2006, 1-5

Lewis, J. A., Neuneck, G., United Nations Institute for Disarmament Research Report, The cyber index, International Security Trends and Realities, Center for Strategic and International Studies, 1-153 <http://www.unidir.org/files/publications/pdfs/cyber-index-2013-en-463.pdf> accessed 17th April 2016 2013

Liberty, No Snoopers Charter, Liberty's Submission to the Joint Committee on the Draft Communications Data Bill 1-39 <http://www.liberty-human-rights.org.uk/pdfs/policy12/liberty-submission-to-the-draft-communications-data-bill-committee-aug-2012-.pdf> accessed 29 June 2014

Liberty, Privacy International, Open Rights Group, Big Brother Watch, Article 19 and English PEN briefing on the fast-track Data Retention and Investigatory Powers Bill, 2014, 1-13 <https://www.liberty-human-rights.org.uk/sites/default/files/Briefing%20on%20the%20Data%20Retention%20and%20Investigatory%20Powers%20Bill.pdf> accessed 19th January 2015

Lin, A. C., Bridging Positivist and Interpretivist Approaches to Qualitative Methods, (26) 1 *Policy Studies Journal* 1998, 162-180

Long, T., Johnson, M., Rigour, reliability and validity in qualitative research, 4 *Clinical Effectiveness in Nursing* 2000, 30-37

Longo, B., Learning on the wires: BYOD, embedded systems, wireless technologies and cybercrime, 13(2) *Legal Information Management* 2013, 119-123

Lowe, D., 'Surveillance and International Terrorism Intelligence Exchange: Balancing the Interests of National Security and Individual Liberty' (2014) *Terrorism and Political Violence*, 1

Lowe, D., Why in Widening Surveillance Powers of Electronic Communications, Co-Operation is needed with Internet and Communications Service Providers, Liverpool John Moores University, 1-19

Luper, S., Epistemic Relativism, 14 *Philosophical Issues Epistemology* 2004, 271-295

Lysnkey, O., Beyond privacy: the data protection implications of the IP Bill, Policy Briefing 15, 2015, 1-4 <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2704299> accessed 1st December 2015

MacEwan, N., A tricky situation: deception in cyberspace, 77(5) *Journal of Criminal Law* 2013, 417-432

MacEwan, N., The Computer Misuse Act 1990: lessons from its past and predictions for its future, 12 *Criminal Law Review* 2008, 955-967

Maguire, M., John, T., 'Intelligence Led Policing, Managerialism and Community Engagement: Competing Priorities and the Role of the National Intelligence Model in the UK' (2006) *Policing and Society* 16(1), 67-85

Marcum, C. D., Higgins, G. E., Ricketts, M. L., Juveniles and Cyber Stalking in the United States: An Analysis of Theoretical Predictors of Patterns of Online Perpetration, 8(1) *International Journal of Cyber Criminology* 2014, 47-56

Marshall, M. N., Sampling for qualitative research, 13(6) *Family Practice* 1996, 522-526

Marx, G. T., 'What's new about the new surveillance? Classifying for change and continuity' (2002) 1(1) *Surveillance and Society*, 9

McCahill, M., 'Theorizing Surveillance in the UK Crime Control Field' (2015) 3(2) *Open Access Journal*, 10-20

McArthur, R. L., Reasonable Expectations of Privacy, 3 *Ethics and Information Technology* 2001, 123-128

McCahill, M., 'Theorizing Surveillance in the UK Crime Control Field' (2015) 3(2) *Open Access Journal*, 10-20

McCosker, H., Barnard, A., Gerber, R., Undertaking Sensitive Research: Issues and Strategies for Meeting the Safety Needs of All Participants, 2(1) *Forum Qualitative Social Research* 2001 <http://www.qualitative-research.net/index.php/fqs/article/view/983/2142> accessed 15 July 2015

McCusker, R., E-commerce, business and crime: inextricably linked, diametrically opposed? 23(1) *Company Lawyer* 2002, 3-8

Mobbs, P., Privacy and Surveillance, How and when organisations and the state can monitor your actions, GreenNet Civil Society Internet Rights Project, 2003, 1-11 <http://www.internetrights.org.uk/briefings/irtb05-rev1-draft.pdf> accessed 29 June 2014

Morris, R. G., Higgins, G. E., Criminological theory in the digital age: The case of social learning theory and digital piracy, 38 *Journal of Criminal Justice* 2010, 470-480

Morse, J., Barrett, M., Mayan, M. M., Olson, K., Spiers, J., Verification strategies for establishing reliability validity in qualitative research, 1(2) *International Journal of Qualitative Methods* 2002, 1–19

Murakami Wood, D., Webster, W., 'Living in surveillance societies: The normalisation of surveillance in Europe' (2009) 5(2) *Journal of Contemporary European Research*, 259

Murphy, M.H., (2016) ‘Transparency and surveillance: assessing the approach of the Investigatory Powers Tribunal in Liberty’ Public Law, Jan, 9-18

Murray, A., Keenan, B., Ensuring the Rule of Law, LSE Law Policy Briefing Series 12, 2015, 1-4 <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2703806> accessed 1st December 2015

Myers, M., Qualitative Research and the Generalizability Question: Standing Firm with Proteus, 4(3-4) *The Qualitative Report* 2000 <http://www.nova.edu/ssss/QR/QR4-3/myers.html> accessed 29th July 2015

Nehaluddin, A., Hackers' criminal behaviour and laws related to hacking, 15(7) *Computer and Telecommunications Law Review* 2009, 159-165

Neuhaus, P. H., Legal Certainty versus Equity in the Conflict of Laws, 28(4) *Law and Contemporary Problems* 1963, 795-807

Newbold, J., 'Predictive Policing', 'Preventative Policing' or 'Intelligence Led Policing'. What is the future? Warwick Business School, 2015, 1-47 <http://library.college.police.uk/docs/Predictive-Preventative-or-Intelligence-Led-Policing.pdf> accessed 2nd September 2017

Nicholls, C., Montgomery, C., Knowles, J. B., Doobay, A., Summers, M., *Nicholls, Montgomery, and Knowles on The Law of Extradition and Mutual* (3rd ed, Oxford, Oxford University Press 2013)

Noble, H., Smith, J., Issues of validity and reliability in qualitative research, 18(2) *Evidence-Based Nursing* 2015, 34-35

Nuth, M. S., Taking advantage of new technologies: For and against crime, 28 *Computer Law & Security Report* 2008, 437-446

O'Connell, N., 'Cyber Security & Data Protection, Roles & Responsibilities' (2016) *Emirates Law Business & Practice*, 16-18

O'Neil, M., Loftus, B., 'Policing and the surveillance of the marginal: Everyday contexts of social control' (2013) 17(4) *Theoretical Criminology*, 437

Ong, B., Standards of proof: is persuading the judge the 'ultimate threshold'? (2010) 5(2) *Construction Law International*, 35-38

Orb, A., Eisenhauer, L., Wynaden, D., Ethics in Qualitative Research, 33(1) *Journal of Nursing Scholarship* 2001, 93-96

Paterson, S., Hopps, B., Lovell, N., United Arab Emirates, Cybersecurity, Herbert Smith Freehills LLP, 17 March 2016, 1-6

Pearsall, B., Predictive Policing: The Future of Law Enforcement? 266 National Institute of Justice Journal 2010, 16-19

Porcedda, M. G., Data Protection and the Prevention of Cybercrime: The EU as an Area of Security? EUI Working Papers, 2012/25, 1-90 <http://cadmus.eui.eu/bitstream/handle/1814/23296/LAW-2012-25.pdf?sequence=1&isAllowed=y> accessed 3rd September 2017

PwC, Economic Crime in the UAE, 2014, 1-6

Rahman, M. M., Khan, M. A., Mohammad, N., Rahman, M. O., Cyberspace claiming new dynamism in the jurisprudential philosophy: a substantive analysis of conceptual and institutional innovation, *International Journal of Law & Management* 2009, 274-289

Roberts, A., Case Comment, R. v Turner (Elliott Vincent): evidence - surveillance, 12 *Criminal Law Review* 2013, 993-995

Roberts, A., Privacy, Data Retention and Domination: Digital Rights Ireland Ltd v Minister for Communications, 78(3) *Modern Law Review* 2015, 535-548

Rychlicki, T., Legal issues of criminal acts committed via botnets, 12(5) *Computer and Telecommunications Law Review* 2006, 161-167

Sah, N., Vinent, V., Cyber attack = armed attack? The implications and the challenges, 19(8) *Computer and Telecommunications Law Review* 2013, 226-233

Sale, J. E. M., Lohfeld, L. H., Brazil, K., Revisiting the Quantitative-Qualitative Debate: Implications for Mixed-Methods Research, 36 *Quality & Quantity* 2002, 43-53

Salgado, M., Data retention - what now? 14(7) *Privacy & Data Protection* 2014, 13-14

Sandelowski, M., Sample size in qualitative research, 18(2) *Research in Nursing & Health* 1995, 179-183

Sarfaraz, H., Surveillance, privacy and cyber law, 20(7) *Computer and Telecommunications Law Review* 2014, 189-194

Schwartz, D. S., A Foundation Theory of Evidence, 100 *Georgetown Law Journal* 2011-2012, 95-172

Shenton, A. K., Strategies for ensuring trustworthiness in qualitative research projects, 22 *Education for Information* 2004, 63-75

Siofra O'Leary (2018) 'Balancing rights in a digital age' *Irish Jurist*, 59, 59-92.

Smith, W. E., Developing a Model Fusion Center to Enhance Information Sharing, PhD Thesis, Naval Postgraduate School, Monterey, California, December 2011, 1-115 <http://www.dtic.mil/dtic/tr/fulltext/u2/a556626.pdf> accessed 3rd September 2017

Skinner, W. F., Fream, A. M., A social learning theory analysis of computer crime among college students, 34 *Journal of Research in Crime and Delinquency* 1997, 495-518

Statewatch, 'Note on big data, crime and security: Civil liberties, data protection and privacy concerns, 3 April 2014, 1-6 <http://www.statewatch.org/analyses/no-242-big-data.pdf> accessed 1st September 2017

Stein, K., 'Unauthorised access' and the UK Computer Misuse Act 1990: House of Lords 'leaves no room' for ambiguity' (2006) 6 *Computer and Telecommunications Law Review,* 63

Suler, J., 'The Online Disinhibition Effect' (2004) 7(3) *Cyberpsychology & Behaviour*, 321-325

Symantec, Internet Security Threat Report, 2013

Symonds, J. E., Gorard, S., The Death of Mixed Methods: Research Labels and their Casualties, The British Educational Research Association, Annual Conference, Heriot Watt University, Edinburgh, 3-6 September 2008, 1-19 <http://www.leeds.ac.uk/educol/documents/174130.pdf> accessed 20th July 2015

Tapper, C., 'Computer crime: Scotch mist?' (1987) *Criminal Law Review* 4

Taylor, N., Policing, privacy and proportionality, *European Human Rights Law Review* 2003, 86-100

T.D.C. Bennet, (2018) 'Judicial activism and the nature of "misuse of private information" Communications Law, 23(2) 74-88

Theohary, C. A., Rollins,, J. W. Cyberwarfare and Cyberterrorism: In Brief, Congressional Research Services, 27 March 2015, 1-15, 2 <https://fas.org/sgp/crs/natsec/R43955.pdf> accessed 3rd September 2017

Tolich, M., Internal confidentiality: When confidentiality assurances fail relational informants, 27 *Qualitative Sociology* 2004, 101–106

Treacy, B., Expert comment, 13(4) *Privacy & Data Protection* 2013, 2

Van den Eynden, V., Corti, L., Woolard, M., Bishop, L., Horton, L., Managing and Sharing Data, 3rd ed, UK Data Archive, May 2011, 1-40 <http://www.data-archive.ac.uk/media/2894/managingsharing.pdf> accessed 1st August 2015

Van Wilsem, J., Hacking and Harassment—Do They Have Something in Common? Comparing Risk Factors for Online Victimization, 29(4) *Journal of Contemporary Criminal Justice* 2013, 437-453

Wasik, M., 'Computer misuse and misconduct in public office' (2008) 22 *International Review of Law, Computers and Technology*, 135

Walden, I., Ramage, S., Computer Crimes and Digital Investigations, Publication Review, 72(1) *Journal of Criminal Law* 2008, 87-88

Walker, D., Brock, D., Stuart, T. R., Faceless-orientated policing: traditional policing theories are not adequate in a cyber world, *Police Journal* 2006, 169-176

Watkins, D., Burton, M., *Research Methods in Law* (Abingdon, Routledge 2013)

Wicks, D., Carney, D., Covert surveillance, Case Comment, 82(2) *Police Journal* 2009, 183-186

Williams, C. A., 'Police Surveillance and the Emergence of CCTV in the 1960s' (2003) 5 *Crime Prevention and Community Safety: An International Journal*, 27-37, 27

Winter, G., A comparative discussion of the notion of validity in qualitative and quantitative research, 4(3-4) *The Qualitative Report* 2000 <http://www.nova.edu/ssss/QR/QR4-3/winter.html> accessed 16th July 2015

World Economic Forum, A Blueprint for Digital Identity, The Role of Financial Institutions in Building Digital Identity, World Economic Forum, August 2016, 1-108

<http://www3.weforum.org/docs/WEF_A_Blueprint_for_Digital_Identity.pdf> accessed 1st September 2017

Yar, M., The Novelty of 'Cybercrime', An Assessment in Light of Routine Activity Theory, 2(4) *European Journal of Criminology* 2005, 407-427

UK House of Lords

House of Lords Debate, 24 November 1997, col 785

Opinions

Communication from Commission to European Parliament: 2000, Creating a Safer Information Society by combating Computer-related Crime <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52000DC0890> accessed 20th January 2015

Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions: Creating a safer information society by improving the security of information infrastructures and combating computer-related crime. COM (2000) 890 final. (Brussels, 2000)

Council of the European Union, General Secretariat, Judgment of the Court of 8 April 2014 in joined Cases C-293/12 and C-594/12, 909/14 JUR, 5 May 2014

European Commission, Data Protection Day 2014: Full Speed on EU Data Protection Reform, 27 January 2014, MEMO/14/60 <http://europa.eu/rapid/press-release_MEMO-14-60_en.htm> accessed 20th January 2015

European Commission, LIBE Committee vote backs new EU data protection rules, 22 October 2013, MEMO/13/923 <http://europa.eu/rapid/press-release_MEMO-13-923_en.htm> accessed 20th January 2015

European Parliament, Minority Opinion pursuant to Rule 48(3) of the Rules of Procedure, A6-0365/2005 final, Report on the proposal for a directive of the European Parliament and of the Council on the retention of data processed in connection with the provision of public electronic communication services and amending Directive 2002/58/EC (COM(2005)0438) - C6-0293/2005 - 2005/0182(COD), 28 November 2005, 1-66 <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A6-2005-0365+0+DOC+PDF+V0//EN> accessed 20th January 2015

Opinion of the European Data Protection Supervisor on the proposal for a Directive of the European Parliament and of the Council on the retention of data processed in connection with the provision of public electronic communication services and amending Directive 2002/58 [2005] OJ C298/1 <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2005:298:0001:0012:EN:PDF> accessed 20th January 2015

Opinion of the European Economic and Social Committee on the Proposal for a Directive of the European Parliament and of the Council on the retention of data processed in connection with the provision of public electronic communication services and amending Directive 2002/58 COM(2005) 438 final--2005/0182 (COD)

Opinion of the Committee on the Internal Market and Consumer Protection for the Committee on Civil Liberties, Justice and Home Affairs on the proposal for a directive

of the European Parliament and of the Council on the retention of data processed in connection with the provision of public electronic communication services and amending Directive 2002/58, COM(2005) 0438 -- C6-0293/2005 -- 2005/0182 (COD)

Siobhan, M, (2016) 'Spying in a Transparent World: Ethics and Intelligence in the 21st Century' Geneva Papers, 19/16 Research Series.

Proposals

European Commission Proposal COM(2005) 438 final, Retention of data processed in connection with the provision of public electronic communication services, 1-17 <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2005:0438:FIN:EN:PDF> accessed 20th January 2015

Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union, 7 February 2013, COM(2013) 48 final

Serious Crime Bill, Explanatory Notes, 2014, 1-85 <http://www.publications.parliament.uk/pa/bills/lbill/2014-2015/0001/en/15001en.pdf> accessed 20th January 2015

Reports

Select Committee on the Constitution, Second Report of Session 2008-09: Surveillance: Citizens and the State, House of Lords Paper No.18-I. (Session 2008-09) 1-130 <http://www.publications.parliament.uk/pa/ld200809/ldselect/ldconst/18/18.pdf> accessed 20th January 2015

All Party Parliamentary Internet Group, Revision of the Computer Act, 2004

Data Protection Working Party (WP29), Statement on the ruling of the Court of Justice of the European Union which invalidates the Data Retention Directive (2014)

European Commission, Evidence for necessity of data retention in the EU, March 2013, 1-29 <http://ec.europa.eu/dgs/home-affairs/pdf/policies/police_cooperation/evidence_en.pdf> accessed 15th December 2015

Home Office Consulting Paper, Interception of Communications in the United Kingdom, Cm 4368. 1999

Home Office, Interception of Communications in the United Kingdom, Cm 4368, 1999

Home Office, Regulation of Investigatory Powers Act 2000 guidance, 18 December 2013, 1-19

<https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/453708/ripa1.pdf> accessed 1st December 2015

Law Commission, Computer Misuse (Working Paper No.110, 1988)

Law Commission's Report No. 186 (Cmnd. 819) 1989Sachstandsbericht Nr. 8: Stand der statistischen Datenerhebung im BKA, 23 June 2011

Secretary of State for the Home Department, Memorandum to the Home Affairs Committee, Post-legislative assessment of the Police and Justice Act 2006, Cm 8195, October 2011, 1-32 <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/229021/8195.pdf> accessed 14th November 2015

Human Rights Council, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Mr Abid Hussain, E/CN.4/2001/64 (Annex V)

United Nations General Assembly, Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Sixty-ninth session, 23 September 2014

Guidance

Codes of Practice and Conduct for forensic science providers and practitioners in the Criminal Justice System, Version 1.0, 2011 <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/118949/codes-practice-conduct.pdf> accessed 2 May 2014

Council of Europe, Economic Crime Division, Cybercrime investigation and the protection of personal data and privacy, 2008, 1-52 <http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/documents/reports-presentations/567%20study5-d-provisional.pdf> accessed 30 June 2014

ENFSI Working Group Forensic IT, Guidelines for Best Practice in the Forensic Examination of Digital Technology 2009, <http://www.enfsi.eu/sites/default/files/documents/forensic_it_best_practice_guide_v6_0.pdf> accessed 2 May 2014

Explanatory Memorandum of the Data Retention and Investigatory Powers Act 2014

House of Lords Science and Technology Committee, Personal Internet Security, Volume I: Report, 5th Report of Session 2006-2007 <http://www.publications.parliament.uk/pa/ld200607/ldselect/ldsctech/165/165i.pdf> accessed 1 July 2014

Human Rights Watch, UAE: Cybercrimes Decree Attacks Free Speech, 28 November 2012 <https://www.hrw.org/news/2012/11/28/uae-cybercrimes-decree-attacks-free-speech> accessed 1st September 2017

Information Commissioner's Officer, Final V 1.0 January 2014, Proposed draft EU General Data Protection Regulation and 'law enforcement' Directive, 2014, 1-19 <http://ico.org.uk/news/blog/2013/~/media/documents/library/Data_Protection/Research_and_reports/Proposed-draft-EU-General-Data-Regulation-and-law-enforcement-Directive-20140124.pdf> accessed 2 May 2014

May, T., Home Secretary, Draft Communications Data Bill, Presented to Parliament by the Secretary of State for the Home Department by Command of Her Majesty, Cm 8359, June 2012, 1-123 <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/228824/8359.pdf> accessed 19th January 2015

Serious Crime Act, Explanatory Notes, 2015, 1-85, para.126 <http://www.legislation.gov.uk/ukpga/2015/9/notes/division/3/2> accessed 23rd August 2015

The Association of Chief Police Officers Good Practice Guide for Digital Evidence 2012, <http://www.acpo.police.uk/documents/crime/2011/201110-cba-digital-evidence-v5.pdf> accessed 2 May 2014

The Association of Chief Police Officers Good Practice Guide for Computer-Based Electronic Evidence, <http://www.7safe.com/electronic_evidence/ACPO_guidelines_computer_evidence.pdf > 2 May 2014

The Association of Chief Police Officers Good Practice Guide for Managers of e-Crime Investigation, <http://www.acpo.police.uk/documents/crime/2011/201103CRIECI14.pdf> accessed 2 May 2014

United Nations Office on Drugs and Crime, Approaches in national cybercrime legislation and the UNODC Cybercrime Repository, undated 1-44 <http://unctad.org/meetings/en/SessionalDocuments/Cybercrime%20Nayelly%20Loya%20(UNODC).pdf> accessed 1st September 2017

Younger Committee, Report on Privacy, 1972

Webpages

aeCert, The Federal Law No. (2) of 2006 on the Prevention of Information Technology Crimes <http://www.aecert.ae/preventionoftechcrimes.php> accessed 29 June 2014

Al Bawaba, Cybercrime laws in the UAE are dangerously vague, 2012 <http://www.thefreelibrary.com/Cyber+crime+laws+in+the+UAE+are+dangerously+vague.-a0308238246> accessed 20th April 2016

Al Lawati, A., UAE internet policies put under the microscope, Gulfnews, 2011 <http://gulfnews.com/news/gulf/uae/media/uae-internet-policies-put-under-the-microscope-1.765600> accessed 30 June 2014

Al Tamimi & Company, Developments in the UAE Cybercrimes Law, The Lawyer 2013 <http://www.thelawyer.com/briefings/developments-in-the-uae-cyber-crimes-law/3004681.article> accessed 20 June 2014

Al Zarooni, M., Most e-crimes from across UAE border, Khaleej Times, 27 September 2013 <http://www.khaleejtimes.com/nation/crime/most-e-crimes-from-across-uae-border> accessed 26th April 2016

Amberhawk, 2011 <http://amberhawk.typepad.com/amberhawk/2011/02/european-commission-explains-why-uks-data-protection-act-is-deficient.html> accessed 3 May 2014

Amnesty International, United Arab Emirates 201/2016 <https://www.amnesty.org/en/countries/middle-east-and-north-africa/united-arab-emirates/report-united-arab-emirates/> accessed 29th April 2016

Ashfords, Cybercrime, 2014 <http://www.ashfords.co.uk/cybercrime/> accessed 1 July 2014

Banck, A. EU Cyber Directive: How does it relate to Data Protection Law and Data Protection Reform? Privacy Europe, 2013 <http://www.privacy-europe.com/blog/eu-cyber-directive-how-does-it-relate-to-data-protection-law-and-data-protection-reform/> accessed 1 July 2014

Baroness Manningham-Buller, Col.297, Parliament.co.uk, 9 December 2008 <http://www.publications.parliament.uk/pa/ld200809/ldhansrd/text/81209-0006.htm#08120935000423> accessed 20th January 2015

Beretta, J., Privacy in the Middle East: new Cybercrime Law, Privacy and Data Security Law, Coverage and commentary on developments in data protection, Dentons, 2013 <http://www.privacyanddatasecuritylaw.com/category/regulators/page/3> accessed 29 June 2014

Black's Law Dictionary <http://thelawdictionary.org/> accessed 20th January 2015

Beretta, J., UAE Issues New Cybercrimes Law and Establishes a National E-Security Authority, Dentons, 7 January 2013 <http://www.dentons.com/en/insights/articles/2013/january/7/uae-issues-new-cyber-crimes-law-and-establishes-a-national-esecurity-authority> accessed 23rd April 2016

Bowcott, O., UK-US surveillance regime was unlawful 'for seven years', The Guardian, 6 February 2015 <https://www.theguardian.com/uk-news/2015/feb/06/gchq-mass-internet-surveillance-unlawful-court-nsa> accessed 28th February 2017

Bowcott, O., GHC surveillance hearing to begin, The Guardian, 14 July 2014 <https://www.theguardian.com/uk-news/2014/jul/14/court-gchq-surveillance-tempora-ipt-nsa-snowden> accessed 1st March 2017

Cadwalladr, C., Edward Snowden: state surveillance in Britain has no limits, Guardian, 12 October 2014 <http://www.theguardian.com/world/2014/oct/12/snowden-state-surveillance-britain-no-limits> accessed 1st December 2014

Cameron, D., Dozens of police-spying tools remain after Facebook, Twitter crack down on Geofeedia, The Daily Dot, 11 October 2016 <https://www.dailydot.com/layer8/geofeedia-twitter-facebook-instagram-social-media-surveillance/> accessed 1st September 2017

Cassim, F., 'Formulating specialised legislation to address the growing spectre of cybercrime: a comparative study' (2009) 12(4) *Scielo* [online]

<http://www.scielo.org.za/scielo.php?script=sci_arttext&pid=S1727-37812009000400004> accessed 27th April 2016

Civic.com, 2017 <https://www.civic.com/> accessed 1st September 2017

Collins, K., UK surveillance law marks a 'worse than scary' shift, CNET, 29 November 2016 <https://www.cnet.com/uk/news/snoopers-charter-investigatory-powers-bill-royal-assent-surveillance-uk/> accessed 1st March 2017

Council of Europe, Action against economic crime, Resources: International cooperation against cybercrime, 2014 <http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Internationalcooperation/default_en.asp> accessed 3 May 2014

Cropper, L., The Investigatory Powers Act 2016 - A "Snoopers' Charter" or a legitimate surveillance tool for today's society, Field Fisher LLP, 2 April 2017 <http://privacylawblog.fieldfisher.com/2017/the-investigatory-powers-act-2016-a-snoopers-charter-or-a-legitimate-surveillance-tool-for-todays-society/> accessed 1st December 2017

Crown Prosecution Service, DPP publishes final guidelines for prosecutions involving social media communications, 20 June 2013 <http://www.cps.gov.uk/news/latest_news/dpp_publishes_final_guidelines_for_prosecutions_involving_social_media_communications/> accessed 20th January 2015

Dajani, H., Sweeping reforms to UAE penal code include harsher penalties and up to Dh1m in fines, The National, 25 October 2016 <http://www.thenational.ae/uae/sweeping-reforms-to-uae-penal-code-include-harsher-penalties-and-up-to-dh1m-in-fines> accessed 15th February 2017

Davidson, M., DRIP: a knee-jerk reaction to the Digital Rights Ireland Ltd decision? Blog.JustCite.com, 18 July 2014 <http://blog.justcite.com/the-drip-bill-a-knee-jerk-reaction-to-the-digital-rights-ireland-ltd-decision> accessed 20 January 2015

Department for Digital, Culture, Media and Sport, 'Data Protection Bill Overview Factsheet', September 2017 https://www.gov.uk/guidance/data-protection-bill-overview <accessed December 2017>

Defense News, UAE to Double Security Budget, Focus on Cyber, 24 February 2014, Military Edge <http://militaryedge.org/articles/uae-double-security-budget-focus-cyber/> accessed 19th April 2016

Digital Identity Summit 2017, The Currency of Trust, 2017 <https://digitalidentitysummit.com/> accessed 2nd September 2017

Dixon M, (2018) 'GDPR should have made cookies toast', Fortune, <http://fortune.com/2018/05/24/gdpr-data-privacy-cookies/> accessed 22 June 2018.

Donaghy, R., Falcon Eye: The Israeli-installed mass civil surveillance system of Abu Dhabi, Middle East Eye, 28 February 2015 <http://www.middleeasteye.net/news/uae-israel-surveillance-2104952769> accessed 29th April 2016

Downton, B., NESA – The New Standard of Information Security in the UAE, MWR InfoSecurity, 6 April 2015 <https://www.mwrinfosecurity.com/articles/nesa-the-new-standard-of-information-security-in-the-uae/> accessed 20th August 2015

Dubai Courts, 2017 <http://www.dubaicourts.gov.ae/portal/page/portal/dc/Legislation_Details?_piref292_457219_292_455214_455214.called_from=1&_piref292_457219_292_455214_455214.law_key=611> accessed 28th February 2017

Ejustice, 2012 <http://ejustice.gov.ae/downloads/latest_laws/cybercrimes_5_2012_en.pdf> accessed 29 June 2014

EPOC Messe Frankfurt GmbH, UAE to face advanced cybercrime in 2013 <http://www.messefrankfurtme.com/frankfurt/1263/for-journalist/technology-production/intersec-middle-east/industry-news/for-journalists.aspx> accessed 15 May 2014

ePrivacy Directive, 2012 <http://eucookiedirective.com/2012/01/11/eprivacy-directive/> accessed 3 May 2014

Eurocrim-database, Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA, 2013 <http://db.eurocrim.org/db/en/vorgang/252/> accessed 1 July 2014

European Central Bank, Forum on the Security of Retail Payments - SecureRe Pay, 2017 <https://www.ecb.europa.eu/paym/pol/forum/html/index.en.html> accessed 2nd September 2017

European Commission Memo, Progress on EU data protection reform now irreversible following European Parliament vote, 2014 <http://europa.eu/rapid/press-release_MEMO-14-186_en.htm> accessed 30 June 2014

European Commission Memo, Data Protection Day 2014: Full Speed on EU Data Protection Reform, 2014 <http://europa.eu/rapid/press-release_MEMO-14-60_en.htm> accessed 30 June 2014

European Commission, Commission proposes a comprehensive reform of the data protection rules, 2012 <http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm> accessed 1st May 2014

European Commission, The EU's Data Protection rules and Cyber Security Strategy: two sides of the same coin, Luxembourg, 19 May 2013 <http://europa.eu/rapid/press-release_SPEECH-13-436_en.htm> accessed 28th April 2016

Europol, A Collective EU Response to Cybercrime, 2015 <https://www.europol.europa.eu/ec3> accessed 20 February 2015

Europol, Cybercrime: A Growing Global Problem, 2014 <https://www.europol.europa.eu/ec/cybercrime-growing> accessed 15 May 2014

Europol, 'Europol enhances cybercrime and internet security cooperation by signing MOU with EURID', 21 December 2016 <https://www.europol.europa.eu/newsroom/news/europol-enhances-cybercrime-and-internet-security-cooperation-signing-mou-eurid> accessed 1st September 2017

Faulkner, A., How to Use Anonymized Global Digital Identities to Fight Cybercrime, RSA Conference, 8 April 2016 <https://www.rsaconference.com/blogs/how-to-use-anonymized-global-digital-identities-to-fight-cybercrime> accessed 1st September 2017

Ferguson, R., Police hold 11 over ransomware scam "affecting thousands, BBC News, 14 February 2013, <http://www.bbc.co.uk/news/technology-21457743> accessed 23 January 2015

Freedom House, United Arab Emirates 2013 <http://www.freedomhouse.org/report/freedom-net/2013/united-arab-emirates#.U7XAKECmWMY> accessed 30 June 2014

Google Spain SL v. Agencia Española de Protección de Datos, 128 *Harvard Law Review* 2014, 735 <http://harvardlawreview.org/2014/12/google-spain-sl-v-agencia-espanola-de-proteccion-de-datos/> accessed 10th August 2015

Gallagher, R., 'European court to decide whether U.K. mass surveillance revealed by Snowden violates human rights', *The Intercept*, 7 November 2017 https://theintercept.com/2017/11/07/uk-surveillance-case-european-court-human-rights/ accessed December 2017

Graux, H., New Directive on Attacks on Information Systems, Time.lex, 2013 <http://www.timelex.eu/en/blog/detail/new-directive-on-attacks-against-information-systems> accessed 1 July 2014

Greenwald, G., UN Reports Finds Mass Surveillance Violates International Treaties and Privacy Rights, The Intercept, 15 October 2014 <https://theintercept.com/2014/10/15/un-investigator-report-condemns-mass-surveillance/> accessed 27th April 2016

Gulf-Law.com, Background on the United Arab Emirates (UAE) Legal System, 2014 <http://gulf-law.com/uaecolaw_legalsystem.html> accessed 3rd April 2016

Gulfnews, Full text of UAE decree on combating cybercrimes, 2012 <http://gulfnews.com/news/gulf/uae/government/full-text-of-uae-decree-on-combating-cyber-crimes-1.1104040> accessed 16 June 2014

Gutwirth, S., Poullet, Y., De Hert, P., *Reinventing Data Protection?* (Springer 2009)

European Parliament News, Q&A on EU data protection reform, 2014 <http://www.europarl.europa.eu/news/en/news-room/content/20130502BKG07917/html/QA-on-EU-data-protection-reform> accessed 30 June 2014

Hill, R., 'UK Data Protection Bill lands: Oh dear, security researchers – where's your exemption?' *The Register*, September 2017 https://www.theregister.co.uk/2017/09/14/messy_data_protection_bill_lands_in_parliament/ accessed December 2017

Hill, R., UK's surveillance regime challenged in landmark European court hearing, *The Register*, November 2017

<https://www.theregister.co.uk/2017/09/14/messy_data_protection_bill_lands_in_parliament/>
accessed December 2017

Hinson, S., Nuclear power on schedule in the United Arab Emirates, Weinberg Foundation, 10 January 2017 <http://www.the-weinberg-foundation.org/2017/01/10/nuclear-power-on-schedule-in-the-united-arab-emirates/> accessed 28th February 2017

Home Office, Police and Criminal Evidence Act 1984 (PACE) codes of practice, 26 March 2013 <https://www.gov.uk/guidance/police-and-criminal-evidence-act-1984-pace-codes-of-practice> accessed 1st December 2015I

Hopkins, R, Interfering with the fundamental rights of practically the entire European population, Panopticon, 10th April 2014 <http://www.panopticonblog.com/2014/04/10/interfering-with-the-fundamental-rights-of-practically-the-entire-european-population/> accessed 21st August 2015

Huhne, C., (2013), 'Prism and Tempora: the cabinet was told nothing of the surveillance state's excesses', The Guardian <https://www.theguardian.com/commentisfree/2013/oct/06/prism-tempora-cabinet-surveillance-state> accessed 25 June 2018

Human Rights Watch, UAE: Cybercrimes Decree Attacks Free Speech, Threatens Peaceful Activists, Ordinary Citizens Alike, 2012 <http://www.hrw.org/news/2012/11/28/uae-cybercrimes-decree-attacks-free-speech> accessed 29 June 2014

Information Commissioner's Office, 2014 <http://ico.org.uk/> accessed 3 May 2014

Information Commissioner's Office, Data Protection, 2014 <https://ico.org.uk/for_organisations/data_protection> accessed 3rd December 2014

Information Commissioner's Office; Data protection principles, 2014 <ico.org.uk/for_organisations/data_protection/the_guide/the_principles> accessed 1 July 2014

International Review of Criminal Policy, United Nations Manual on the Prevention and Control of Computer-Related Crime, Nos.43-44 , 1999 <http://www.uncjin.org/Documents/irpc4344.pdf> accessed 20th January 2015

Iaccino, L., UAE cybercrime: Man faces £42,000 fine for swearing at colleague over WhatsApp, International Business Times, 18 June 2015 <http://www.ibtimes.co.uk/uae-cybercrime-man-faces-42000-fine-swearing-colleague-over-whatsapp-1506803> accessed 22nd August 2015

ITP.net, UAE cyber-security authority unveils policies, standards, 2014 <http://www.itp.net/598777-uae-cyber-security-authority-unveils-policies-standards> accessed 29 June 2014

Indonesian Embassy, Indonesia and UAE signed Agreement and Extradition and Mutual Legal Assistance, 3 February 2014 <http://indonesianembassy.ae/indonesia-uae-signed-extradition-agreement-and-mutual-legal-assistance/> accessed 28th February 2017

Jenkins, S., Blanket digital surveillance is a start. But how about a camera in every bathroom? The Guardian, 17 July 2014 <http://www.theguardian.com/commentisfree/2014/jul/17/blanket-digital-surveillance-is-a-start-but-how-about-a-camera-in-every-bathroom> accessed 25th April 2016

Jones, S., Global Dispatches: UAE - A Guide for Internet Use in the UAE, The Epoch Times, 2010 <http://www.theepochtimes.com/n2/opinion/uae-internet-united-arab-emirates-blckberry-google-government-42724.html> accessed 30 June 2014

Keane, J., This ain't CSI: How the FBI Hunts Down Cyber Criminals Around the Globe, Digital Trends, 2 August 2015 <http://www.digitaltrends.com/computing/how-the-fbi-hunts-down-cyber-criminals-around-the-globe/> accessed 29th April 2016

Kelly, J. X., Computer Misuse Overview, JISC Legal Information, 2007 <http://www.jisclegal.ac.uk/LegalAreas/ComputerMisuse/ComputerMisuseOverview.aspx> accessed 17 June 2014

Khasawneh, N. A., Ahern, G., Cybercrimes law - United Arab Emirates, Eversheds LLP, 5 December 2012 < http://www.lexology.com/library/detail.aspx?g=62f0c34f-0d12-4bbe-bb93-decfc71d4105> accessed 20th January 2015

Kiss, J., Academics: UK 'Drip' data law changes are 'serious expansion of surveillance', The Guardian, 15 July 2014 <http://www.theguardian.com/technology/2014/jul/15/academics-uk-data-law-surveillance-bill-rushed-parliament> accessed 15th December 2015

Lambert, D., 'Intelligence-Led Policing in a Fusion Center', Federal Bureau of Investigation, December 2010 <https://leb.fbi.gov/2010/december/intelligence-led-policing-in-a-fusion-center> accessed 1st September 2017

Liberty, Summary of Surveillance Powers Under RIPA, 2010, 1-17 <http://www.liberty-human-rights.org.uk/materials/introduction-to-ripa-august-2010.pdf> accessed 29 June 2014

Macaskill, E., 'Extreme surveillance' becomes UK law with barely a whimper, 19 November 2016 <https://www.theguardian.com/world/2016/nov/19/extreme-surveillance-becomes-uk-law-with-barely-a-whimper> accessed 28th February 2017

Mainelli, M., Blockchain will help us prove our identities in a digital world, Harvard Business Review, 16 March 2017 <https://hbr.org/2017/03/blockchain-will-help-us-prove-our-identities-in-a-digital-world> accessed 1st September 2017

Malek, C., UAE needs better protection of critical infrastructure, The National, 19 November 2014 <http://www.thenational.ae/uae/technology/uae-needs-better-protection-of-critical-infrastructure> accessed 22nd August 2015

Martin, A. J., UK gov says new Home Sec will have powers to ban end-to-end encryption, The Register, 14 July 2016 <https://www.theregister.co.uk/2016/07/14/gov_says_new_home_sec_iwilli_have_powers_to_ban_endtoend_encryption/> accessed 1st March 2016

McAuley, A., UAE nuclear project enters critical phase, the National, 7 July 2015 <http://www.thenational.ae/business/energy/uae-nuclear-project-enters-critical-phase> accessed 20th April 2016

McBride, S., HH Sheikh Khalifa issues decree on cybercrime, ITP.net, 13 November 2012 <http://www.itp.net/591227-hh-sheikh-khalifa-issues-decree-on-cyber-crime> accessed 23rd January 2015

Megget, K., Hong Kong, Singapore and UAE main hubs for fake trade, Securing Industry, 23 June 2017 <https://www.securingindustry.com/hong-kong-singapore-and-

uae-main-hubs-for-fake-trade/s111/a4881/#.Wbxc89HTXIU> accessed 2nd September 2017

ME-Newswire, Cybercrimes Conference recommends establishing specialized prosecutions in federal and local courts, Abu Dhabi, UAE, 5 April 2014 <http://www.me-newswire.net/news/cyber-crimes-conference-recommends-establishing-specialized-prosecutions-in-federal-and-local-courts/en> accessed 26th April 2016

Merriam Dictionary <http://www.merriam-webster.com/dictionary/privacy> accessed 20th January 2015

Millar, S., Norton-Taylor, R., Black, I., Worldwide spying network is revealed, The Guardian, 26 May 2001 <https://www.theguardian.com/uk/2001/may/26/richardnortontaylor.ianblack> accessed 1st September 2017

Mustafa, A., UAE to Double Security Budge, Focus on Cyber, Defense News, 2014 <http://www.defensenews.com/article/20140224/DEFREG04/302240015/UAE-Double-Security-Budget-Focus-Cyber> accessed 30 June 2014

Norton Rose, Key data privacy and intellectual property issues in the UAE, November 2011 <http://www.nortonrosefulbright.com/knowledge/publications/54334/key-data-privacy-and-intellectual-property-issues-in-the-uae> accessed 20th January 2015

O'Connell, N., Data Protection and Privacy Issues in the Middle East, Tamimi, 12/13 December 2011 <http://www.tamimi.com/en/magazine/law-update/section-6/january-february-1/data-protection-and-privacy-issues-in-the-middle-east.html> accessed 20th January 2015

OpenNet Initiative, Internet Filtering in the United Arab Emirates in 2006-2007, 2007 <https://opennet.net/studies/uae2007> 30 June 2014

Out-Law.com, EU data retention rules unlawful, rules CJEU, 8 April 2014 <http://www.out-law.com/en/articles/2014/april/eu-data-retention-rules-unlawful-rules-cjeu/> accessed 23rd August 2015

Parker, A., Address by the Director-General of the Security Service to the Royal United Services Institute at Thames House, Security Service MI5, 8th January 2015, 2015 <https://www.mi5.gov.uk/home/about-us/who-we-are/staff-and-management/director-general/speeches-by-the-director-general/director-generals-speech-on-terrorism-technology-and-accountability.html> accessed 1st December 2015

Parliament, Chapter 4: Legal Regulation and Safeguards, 2009 <http://www.publications.parliament.uk/pa/ld200809/ldselect/ldconst/18/1806.htm> accessed 2 May 2014

Parliament UK, Fifty-ninth Report of Session 2010-12 - European Scrutiny Committee, Data processing in the framework of police and criminal cooperation <http://www.publications.parliament.uk/pa/cm201012/cmselect/cmeuleg/428-liv/42810.htm> accessed 1 July 2014

Parliament UK, Serious Crime Bill [HL] 2014-15 <http://services.parliament.uk/bills/2014-15/seriouscrime.html> accessed 1 July 2014

Pinsent Masons, US to strengthen Safe Harbour framework for personal data transfers from EU by summer, Out-Law.com, 2014 <http://www.out-law.com/en/articles/2014/march/us-to-strengthen-safe-harbour-framework-for-personal-data-transfers-from-eu-by-summer/> accessed 15 June 2014

Practical Law, Data protection in United Arab Emirates: overview, 1 April 2014 <http://uk.practicallaw.com/0-518-8836#> accessed 20th January 2015

Privacy International, Investigatory Powers Tribunal rules GCHQ mass surveillance programme TEMPORA is legal in principle, 18 December 2014 <https://www.privacyinternational.org/node/46> accessed 1st March 2017

Reding, V., The EU's Data Protection rules and Cyber Security Strategy: two sides of the same coin, European Commission, 2013 <http://europa.eu/rapid/press-release_SPEECH-13-436_en.htm> accessed 30 June 2014

Reporters without Borders, United Arab Emirates: Tracking "cyber-criminals", 2014 <http://12mars.rsf.org/2014-en/2014/03/11/united-arab-emirates-tracking-cyber-criminals/> accessed 30 June 2014

Ryder, M., Case Preview: Al-Rawi v Security Service, Tariq v Home Office, UK Supreme Court Blog, 2 March 2012 <http://ukscblog.com/case-preview-al-rawi-v-security-service-tariq-v-home-office/> accessed 15th August 2015

Saab, Saab receives order for new advanced airborne surveillance systems from UAE, 10 November 2015 <http://saabgroup.com/media/news-press/news/2015-11/saab-receives-order-for-new-advanced-airborne-surveillance-systems-from-uae/> accessed 28th April 2016

Sadowski, J., Police data could be labelling 'suspects' for crimes they have not committed, The Guardian, 4 February 2016 <https://www.theguardian.com/technology/2016/feb/04/us-police-data-analytics-smart-cities-crime-likelihood-fresno-chicago-heat-list> accessed 1st March 2017

Saleem, S., New Law Combating Information Technology crimes, 2013, Tamimi <http://www.tamimi.com/en/magazine/law-update/section-5/january-2/new-law-combating-information-technology-crimes.html> accessed 21st April 2016

Samoglou, E., UAE researcher calls for more stringent cyber security, The National, 1 April 2015 <http://www.thenational.ae/uae/technology/uae-researcher-calls-for-more-stringent-cyber-security> accessed 24th February 2017

Shubber, K., A simple guide to GCHR's internet surveillance programme Tempora, Wired, 24 June 2013 <http://www.wired.co.uk/news/archive/2013-06/24/gchq-tempora-101> accessed 14th December 2015

Snowden, E., What Europe Should Know about US Mass Surveillance, Whistleblower delivers written testimony to European Parliament (*Original.antiwar.com,* 2014) <http://original.antiwar.com/edward-snowden/2014/03/07/what-europe-should-know-about-us-mass-surveillance/> 30 April 2014

Stanford Encyclopedia of Philosophy, Logic and Ontology, 2011 <http://plato.stanford.edu/entries/logic-ontology/#DifConOnt> accessed 18 June 2014

Statewatch, 'Note on big data, crime and security: Civil liberties, data protection and privacy concerns, 3 April 2014, 1-6, 6 <http://www.statewatch.org/analyses/no-242-big-data.pdf> accessed 1st September 2017

Stupp, C., EU to propose new rules targeting encrypted apps in June, 29 March 20017 <https://www.euractiv.com/section/data-protection/news/eu-to-propose-new-rules-on-police-access-to-encrypted-data-in-june/> accessed 1st September 2017

Telecommunications Regulatory Authority <http://www.tra.org.aw> accessed 17th April 2016

Timm, T., The government just admitted it will use smart home devices for spying, The Guardian, 9 February 2016 <https://www.theguardian.com/commentisfree/2016/feb/09/internet-of-things-smart-devices-spying-surveillance-us-government> accessed 2nd September 2017

Thomas, B., UAE Military To Set Up Cyber Command, Defenseworld.net, 30 September 2014 <http://www.defenseworld.net/news/11185/UAE_Military_To_Set_Up_Cyber_Command#.VMVEmywsq6Q> accessed 20th January 2015

Travis, A., Investigatory powers bill: snooper's charter to remain firmly in place, The Guardian, 2 November 2015 <http://www.theguardian.com/world/2015/nov/02/investigatory-powers-bill-snoopers-charter-will-remain-firmly-in-place> accessed 1st December 2015

Travis, A., 'Snooper's charter' bill becomes law, extending UK state surveillance, The Guardian, 29 November 2016 <https://www.theguardian.com/world/2016/nov/29/snoopers-charter-bill-becomes-law-extending-uk-state-surveillance> accessed 1st December 2017

Turner, M., Pantlin, N., Pugh, L., Young, C., EU Cybercrime Directive takes a tougher stance against attacks on information systems, Herbert Smith Freehills LLP, 2013 <http://www.lexology.com/library/detail.aspx?g=d3863b21-3c3b-419e-8a8f-2b007acb3a10> accessed 1 July 2014

UAE Computer Emergency Response Team <https://www.tra.gov.ae/aecert/en/media/news-archive/2015/3/31/the-tras-uae-computer-emergency-response-team-aecert-organizes-an-aviation-security-workshop.aspx> accessed 20th April 2016

UAE Interact, UAE and Italy sign two agreements on judicial cooperation, 18 September 2015 <http://www.uaeinteract.com/docs/UAE_and_Italy_sign_two_agreements_on_judicial_cooperation/71128.htm> accessed 28th February 2017

UK Cyber Security Strategy, Protecting and promoting the UK in a digital world, November 2011, 1-43 <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf> accessed 3rd December 2014

UK Government, Foreign travel advice, United Arab Emirates, Terrorism, 2017 <https://www.gov.uk/foreign-travel-advice/united-arab-emirates/terrorism> accessed 28th February 2017

Valenzuela, D., Shrivastava, P., Interview as a Method for Qualitative Research, 1-20 <http://www.public.asu.edu/~kroel/www500/Interview%20Fri.pdf> accessed 3 May 2014

Vincent, J., The UK now wields unprecedented surveillance powers - here's what it means, The Verge, 29 November 2016 <https://www.theverge.com/2016/11/23/13718768/uk-surveillance-laws-explained-investigatory-powers-bill> accessed 1st September 2017

Vitaris, B., Swiss "Crypto Valley" to Create Digital Identities for Its Citizens on the Ethereum Blockchain, Bitcoin Magazine 13 July 2017 <https://bitcoinmagazine.com/articles/swiss-crypto-valley-create-digital-identities-its-citizens-ethereum-blockchain/> accessed 3rd September 2017

Walker, C., EU rules on breach notification, Olswang, 2014 <http://www.olswang.com/articles/2014/06/eu-rules-on-breach-notification/> accessed 1 July 2014

WAM, UAE, Australia sign two extradition and legal assistance treaties, 30 July 2007 <http://wam.ae/en/details/1395227894411> accessed 28th February 2007

WAM, Telecommunications Regulatory Authority prevents 289 cyber-attacks in Q1 2017, Emirates247, 31 July 2017

<http://www.emirates247.com/news/emirates/telecommunications-regulatory-authority-prevents-289-cyber-attacks-in-q1-2017-2017-07-31-1.656939> accessed 1st December 2017

10. Appendices

10.1.1 Interview Schedules

The main interview questions are numbered and follow-up questions/prompts are alphabetized.

MIDDLESEX UNIVERSITY

INTERVIEW GUIDE UAE JUDGE

Icebreaker question (Research objective 5)

1. Could you tell me about your professional career?

    a) How long have you been a judge and dealt with cybercrime?

    b) Does the area of cybercrime pose specific challenges for judges?

    c) If so, which ones?

    d) In general, is it more difficult to be a judge in the area of cybercrime?

2. In your opinion, should more cybercrime offences be adopted than those set out in Federal Law No.2 of 2006 on combating cybercrime and Law No. 5 of 2012 Concerning Combating Information Technology Crimes? UAE cybercrime offences legislation (Research objective 5)

    a) If so, what type of cybercrime offences should be adopted?

    b) Do certain cyber criminals escape punishment and if so, why?

    c) Do you think that the existing cybercrime offences are sufficient to prosecute cyber criminals which target critical infrastructure?

3. Do you think that the issue of extra-territorial jurisdiction is sufficiently addressed by the existing cybercrime legislation? UAE cybercrime legislation (Research objective 5)

a) If not, why not?

b) Should territorial jurisdiction be extended to close potential gaps in jurisdictional reach?

c) In your opinion, what should be the basis for this, for instance, prescriptive jurisdiction in accordance with the nationality principle (i.e. jurisdiction for acts committed by nationals irrespective of location) or objective territoriality (i.e. jurisdiction for acts committed even outside the jurisdiction but which affect the UAE) or both?

4. In your experience, what would you consider to be the greatest problem for judges hearing cybercrime cases? UAE cybercrime framework (Research objective 5)

a) To what extent can that problem be addressed?

b) Do you think that there are any legislative gaps within the cybercrime legislative framework which cause problems?

c) What problems do these other legislative gaps cause?

d) How can these be addressed?

5. What is your opinion about surveillance powers in the fight against cybercrime and current problems with the law? Surveillance (Research objective 5)

a) Do you agree that the current legislative framework fails to adequately address surveillance powers (i.e. does not spell out the powers for enforcement personnel in respect of interception, surveillance, communications data acquisition and decryption)?

b) Do you think that enforcement personnel require more comprehensive and invasive powers to collect information?

c) What do you think about interception of communications and bulk collection of communications data?

d) What is your opinion about data acquisition powers in the fight against cybercrime and current problems with the law?

e) What steps can be taken to prevent abuse of broad enforcement powers?

6. Should the UAE adopt a law requiring communication service providers to retain data? Data retention (Research objective 5)

a) How long should communication service providers be required to retain data?

b) What sort of data should be retained?

7. What is your opinion about decryption powers in the fight against cybercrime and current problems with the law? Surveillance (Research objective 5)

a) Do you think the law should ban encryption or require companies to open a backdoor for enforcement personnel to easily access encrypted content?

b) If so, why?

8. Do you think that the UAE should improve its data protection laws? Data protection (Research objective 5)

a) If so, why?

b) What data protection reform is needed to improve cyber security?

c) In your opinion, how can a balance be struck between protecting the public and using surveillance, interception and data retention, decryption and protecting the right to privacy?

9. How can evidence laws be improved in respect of cybercrimes? Evidence rules on the admissibility of digital evidence and intercept material in criminal proceedings (Research objective 5)

a) What would you consider to be the greatest problem with the current evidence laws in respect of cybercrimes?

b) What other problems exist?

c) Is there a problem with considering intercept material not admissible in criminal proceedings?

d) Do you think that evidence rules should be developed for digital evidence and intercept material?

10. Do you have any other legislative improvement suggestions?

MIDDLESEX UNIVERSITY

INTERVIEW GUIDE UAE PROSECUTORS

Icebreaker question (Research objective 5)

1. Could you tell me about your professional career?

    a) How long have you been a prosecutor and dealt with cybercrime?

    b) Does the area of cybercrime pose specific challenges for prosecutors?

    c) If so, which ones?

    d) In general, is it more difficult to be a prosecutor in the area of cybercrime?

2. In your opinion, should more cybercrime offences be adopted than those set out in Federal Law No.2 of 2006 on combating cybercrime and Law No. 5 of 2012 Concerning Combating Information Technology Crimes? UAE cybercrime offences legislation (Research objective 5)

    a) If so, what other cybercrime offences should be adopted?

    b) Do certain cyber criminals escape prosecution and if so, why?

    c) Do you think that the existing cybercrime offences are sufficient to prosecute cyber criminals which target critical infrastructure?

3. Do you think that the issue of extra-territorial jurisdiction is sufficiently addressed by the existing cybercrime legislation? UAE cybercrime legislation (Research objective 5)

    a) If not, why not?

b) Should jurisdiction be extended to close potential gaps in jurisdictional reach when prosecuting individuals who are not located in the UAE?

c) How should the law address this?

4. In your experience, what would you consider to be the greatest problem for prosecutors dealing with cybercrime cases? UAE cybercrime framework (Research objective 5)

a) To what extent can that problem be addressed?

b) Do you think that there are any other legislative gaps within the cybercrime legislative framework which cause problems?

c) What problems do these other legislative gaps cause?

d) How can these be addressed?

5. What is your opinion about surveillance powers in the fight against cybercrime and current problems with the law? Surveillance (Research objective 5)

a) Do you agree that the current legislative framework fails to adequately address surveillance powers (i.e. does not spell out the powers for enforcement personnel in respect of interception, surveillance, communications data acquisition and decryption)?

b) Do you think that enforcement personnel require more comprehensive and invasive powers to collect information?

c) What do you think about interception of communications and bulk collection of communications data?

d) What is your opinion about data acquisition powers in the fight against cybercrime and current problems with the law?

e) What steps can be taken to prevent abuse of broad enforcement powers?

6. Should the UAE adopt a law requiring communication service providers to retain data? Data retention (Research objective 5)

a) How long should communication service providers be required to retain data?

b) What sort of data should be retained?

7. What is your opinion about decryption powers in the fight against cybercrime and current problems with the law? Surveillance (Research objective 5)

a) Do you think the law should ban encryption or require companies to open a backdoor for enforcement personnel to easily access encrypted content?

b) If so, why?

8. Do you think that the UAE should improve its data protection laws? Data protection (Research objective 5)

a) If so, why?

b) What data protection reform is needed to improve cyber security?

c) In your opinion, how can a balance be struck between protecting the public and using surveillance, interception and data retention, decryption and protecting the right to privacy?

9. How can evidence laws be improved in respect of cybercrimes? Evidence rules on the admissibility of digital evidence and intercept material in criminal proceedings (Research objective 5)

a) What would you consider to be the greatest problem with the current evidence laws in respect of prosecuting cyber criminals?

b) What other problems exist?

c) Is there a problem with considering intercept material inadmissible in criminal proceedings?

10. Do you have any other suggestions on how to improve the prosecution of cyber criminals? The UAE's legislative framework to combat e-crime (Research objective 5)

a) Do you have any other suggestions to improve the UAE's legislative framework to combat e-crime?

MIDDLESEX UNIVERSITY

INTERVIEW GUIDE Interpol

1. Could you tell me about your professional career?
    a) How long have you worked for Interpol and dealt with cybercrime?
    b) Does the area of cybercrime pose specific challenges?
    c) If so, which ones?.
    d) In general, is it more difficult to work for Europol in the area of cybercrime?

2. On a policy level, what measures are important to strategically combat cybercrime? (Research objective 3)

3. In your opinion, what are the key requirements for a successful domestic and regional cybercrime strategy (Research objective 3)

4. In your experience, what would you consider to be the greatest problem for Europol and national law enforcement agencies when combating cybercrime? (Research objective 3)
    a) To what extent can that problem be addressed?
    b) What other operational problems exist?
    c) Are there any preventative related issues?
    d) If so, which ones are there?

5. How important are surveillance powers in the fight against cybercrime? Surveillance (Research objective 2)
    a) In your opinion, how far-reaching should interception, surveillance, communications data acquisition and decryption of data be?
    b) In practice, how does mass surveillance work?
    c) What sort of set up is required for mass surveillance?

6. How essential is data retention by communication service providers? (Research objective 2)
    a) What type of data is most important for Europol and law enforcement agencies?
    b) In your opinion, how long should data be retained?

7. Do you consider it a good strategy to weaken or ban encryption or in the alternative to require that backdoors are created for law enforcement officers? (Research objective 2)
    a) Do you prefer a ban on encryption over backdoors for law enforcement officers?
    b) Do you think that there are problems with a ban on encryption and/or the creation of backdoors?
    c) If so, which ones?
    d) In your opinion, to which extent can these be addressed?

8. How can network and information security be best achieved? (Research objective 3)

9. In your opinion, what role does privacy and data protection play in ensuring network and information security?

10. How can the right balance be struck in cyberspace between privacy and security.

11. Do you have any other suggestions to improve the legislative framework to combat e-crime? (Research objective 3)

MIDDLESEX UNIVERSITY

INTERVIEW GUIDE UAE POLICE OFFICER

Icebreaker question (Research objective 5)

1. Could you tell me about your professional career?

    a) How long have you worked as a police officer and dealt with cybercrime?

    b) Does the area of cybercrime pose specific challenges for police officers?

    c) If so, which ones?

    d) In general, is it more difficult to be a police officer in the area of cybercrime?

2. In your opinion, should more cybercrime offences be adopted than those set out in Federal Law No.2 of 2006 on combating cybercrime and Law No. 5 of 2012 Concerning Combating Information Technology Crimes? UAE cybercrime offences legislation (Research objective 5)

    a) If so, what type of cybercrime offences should be adopted?

    b) Do certain cyber criminals escape punishment and if so, why?

    c) Do you think that the existing cybercrime offences are sufficient to prosecute cyber criminals which target critical infrastructure?

3. When cybercrime is committed in the UAE by individuals who are located abroad, are there are operational issues?

    a) To what extent are these overcome?

    b) In your opinion, how can these problems be addressed?

c) Do you think that jurisdiction should be further extended?

4. In your experience, what would you consider to be the greatest problem for police officers combating cybercrime? Network and information security (Research objective)

a) To what extent can that problem be addressed?

b) What other operational problems exist?

c) Are there any preventative related issues?

d) If so, which ones are there?

e) How can these be addressed?

5. What is your opinion about surveillance powers in the fight against cybercrime? Surveillance (Research objective 5)

a) Do you agree that the current legislative framework fails to give police officers adequate surveillance powers (i.e. does not spell out the powers for enforcement personnel in respect of interception, surveillance, communications data acquisition and decryption)?

b) Do you think that the police require more comprehensive and invasive powers to collect information?

c) What do you think about interception of communications and bulk collection of communications data?

d) How extensive should data collection be i.e. what data should be collected by communications service providers?

e) What role should mass surveillance play in the fight against cybercrime?

f) In practice, how would mass surveillance work?

g) What do you think about interception of social networks?

h) What steps can be taken to prevent abuse of broad policing powers?

6. Should the UAE adopt a law requiring communication service providers to retain data? Data retention (Research objective 5)

a) How long should communication service providers be required to retain data?

b) What sort of data should be retained?

7. What do you think about requiring communication service providers to assist with communications interference and interception and to require them to retain the ability to decrypt data? Surveillance (Research objective 5)

a) Do you consider it a good strategy to weaken or ban encryption?

b) In the alternative, should law enforcement officers be given easy access i.e. by requiring that backdoors are created?

c) If so, why?

8. How can network and information security be best achieved? Data protection and network and information security (Research objective 5)

a) In your opinion, what role should privacy and data protection play in ensuring network and information security?

9. Have you encountered problems with current evidence rules on the admissibility of digital evidence and intercept material in criminal proceedings laws in respect of cybercrimes? Evidence rules on the admissibility of digital evidence and intercept material in criminal proceedings (Research objective 5)

a) Which type of problems did you come across?

b) In your opinion, how can these be addressed?

10. Do you have any other suggestions, so that the police can combat cybercrime more effectively in the UAE? (Research objective 5)

a) Do you have any other suggestions to improve the UAE's legislative framework to combat e-crime?

MIDDLESEX UNIVERSITY

INTERVIEW GUIDE FOR EMPLOYEE OF UAE COMPANY

Research objective 5 (Icebreaker question)

1. Could you tell me about your professional career?

    a) How long have you worked in cyber security at your current employer?

    b) Why did you choose this field?

    c) What particular challenges do you face?

2. What problems have you encountered when dealing with cybercrime and security related issues at your company? Cyber-crime offences (Research objective 5)

    a) What would you consider to be the greatest problem?

    b) To what extent can that problem be addressed?

    c) Do you think that these challenges are also attributable to legislative gaps within the cybercrime offences framework?

    d) If so, what legislative gaps do you think exist?

    e) What problems do these legislative gaps cause?

3. In your opinion, what role should the private sector play in assisting law enforcement with surveillance? Surveillance through private sector cooperation (Research objective 5)

    a) Should the private sector undertake mass surveillance for the government?

4. Is encryption important for your company? Encryption and security (Research objective 5)

a) Is it important for enterprise IT security?

b) Do you consider a ban on encryption would expose your company to security risks?

c) If so, why?

d) Do you think that creating backdoors for enforcement personnel to access encrypted content, including of commercial data, is a good or bad idea?

e) If so, why?

5. How does your company ensure data protection? Data protection (Research objective

a) What processes are in place to ensure that personal data is protected?

b) In your opinion, how can data protection be improved in the UAE?

c) Do you think that it is a good idea if companies which handle personal data had to notify security or data protection breaches to the authorities?

6. From your experience, what steps should the UAE take to improve cyber security and to combat cybercrime? Network and information security laws (Research objective 5)

a) Are different laws needed and if so, what types of laws?

c) What can the UAE do to create a more stable digital environment for businesses operating in the UAE?

7. Do you have any other suggestions to improve the UAE's legislative framework to combat e-crime? UAE's legislative framework to combat e-crime (Research objective 5)

10.1.2 Interview Information Sheet and Consent Form

24 October 2016

To Whom It May Concern

This letter confirms that Mr. Waleid Alantali is a doctoral candidate in the School of Law at the University of Middlesex in London (United Kingdom). He is in the process of writing his doctoral thesis and he is collecting data for that purpose. The doctoral thesis explores Strengthening e-crime legislation in the UAE: Learning lessons from the UK and the EU.

Interviews will be conducted in United Arab Emirates, from October to December 2016. He is planning to interview key personnel in government bodies who deal with e-crime legislation such as judges, enforcement agencies, the office of prosecution, the secret service and companies operating in the UAE.

The data collected will be anonymised in order to ensure the confidentiality of participant's views and information provided.

The purpose of this letter is to ask for your assistance by agreeing to be a participant in this study.

Yours sincerely,

Julia C. Davidson

Julia Davidson, PhD
Professor of Criminology
Co-Director Centre for Abuse & Trauma Studies
Middlesex University
The Burroughs, Hendon,
London NW4 4BT

Middlesex University London

CONSENT FORM

Strengthening e-crime legislation in the UAE: Learning lessons from the UK and the EU

Please read the participant information sheet and if you are willing to participate, please kindly read the below form and initial it.

Please Read and Initial the Boxes

1. I have read the attached participant information sheet about the research and could consider the topic. I was able to raise questions and have them answered adequately. ☐

2. I have been made aware that participation is voluntary and that I can withdraw my consent to participate without having to provide any reason and at any time. ☐

3. I am happy that an audio-record is made of the interview. ☐

4. I give my consent that the researcher can quote what I say, so long as it is ensured that I cannot be identified as a result of it. ☐

I agree to take part in the research about strengthening e-crime legislation in the UAE: Learning lessons from the UK and the EU.

Name of research participant in capital letters:

Date:

Signature:

10.1.3 Example of an Interview Request to a UK Expert

From: waleid al antali [mailto:xwaleidx@hotmail.com]
Sent: 23 July 2017 23:28
To: Communication
Subject: PhD research

Dear Sirs,

I am a PhD student at Middlesex University London, whose field of research is how to strengthen e-crime legislation. As part of my doctoral research, I intend to interview a police officer specialised in the field of cybercrime. I would be most obliged if you can point me in the right direction and could inform me whom I could make contact with in order to arrange an interview, either in person, by phone or via Skype. In the alternative, I could also email the questions and any of them could be answered in writing.

I highly appreciate the assistance with this matter, which is also in the public interest since it will contribute to the available knowledge in the field.

I look forward to hearing from you.

Yours faithfully,
Waleid Alantali

10.1.4 Response Received from a UK Expert to an Interview Request

From: NCCU Strategy <nccu.strategy@ncax.gsi.gov.uk>
Date: July 28, 2017 at 6:06:34 PM GMT+4
To: "xwaleidx@hotmail.com" <xwaleidx@hotmail.com>
Cc: NCCU Strategy <nccu.strategy@nca.x.gsi.gov.uk>
Subject: RE: PhD research

OFFICIAL

Dear Waleid,

Many thanks for your enquiry. Unfortunately, we're not able to help on this occasion, but you may find the information on our website helpful for your research.

Best wishes,

Threat Response, NCCU

Threat Response
National Cybercrime Unit
National Crime Agency
www.nationalcrimeagency.gov.uk
www.facebook.com/NCA
Twitter: @NCA_UK