Is Internet privacy dead? Recovering Internet privacy in an increasingly surveillant society.

Jeremy Michael Harmer

Submitted in accordance with the requirements for the degree of
Doctor of Philosophy

The University of Leeds
School of Law

January, 2017

The candidate confirms that the work submitted is his own and that appropriate credit has been given where reference has been made to the work of others.

Acknowledgements

This thesis concludes 8 years and 7 months of research (including 2 extensions given on medical grounds) as a part-time Ph.D. student in School of Law at the University of Leeds.

First and foremost, I am grateful to my employer - IT Services at the University of Leeds - for subsidising part of my academic fee and allowing me 5 days study leave from work annually to conduct and complete this doctoral research.

I would also like to express my greatest thanks to my supervisors, Dr. Subhajit Basu and Mr. Nick Taylor, for supervision and understanding and encouraging me at critical stages of my research. I am grateful to have had the opportunity to benefit from their academic guidance, motivation, encouragement and support. Also, I would like to express my thanks and appreciation to Dr. Yaman Akdeniz for his guidance and support during the first few months of my research.

I would especially like to thank my wife Yim Ling and my two children for their endless support and understanding, in particular through stressful times and my ill health.

Abstract

Surveillance on the Internet is a new battleground which attracts attention from all walks of life in our society. Since the 2013 Snowden revelations, the practice of Internet surveillance has become common knowledge. This research critically examines whether or not Internet privacy is dead, with a specific focus on the technical aspects of the Internet in order to express how technology is used to enhance and to invade privacy. This sets it apart from the existing literature in the field.

In this research, three jurisdictions are chosen as case studies: the US and the UK as western jurisdictions with different legal systems, and China which has extensive surveillance and limited Internet privacy. The research explores the meaning of privacy in the information society and investigates the ways in which Internet privacy is integrated in the three chosen jurisdictions are critically analysed and discussed.

The research findings reveal that Internet privacy is being taken away in both the US and the UK and it is hard to be optimistic for the future in the light of the 2013 Snowden revelations and ongoing changes to legislation, particularly the Investigatory Powers Bill in the UK. Through the examination of the evolution of the Internet in China and its nascent and evolving laws relating to data protection and privacy, the research findings demonstrate that China holds a great deal of control over its Internet and has implemented technical measures of surveillance, effectively meaning that Internet privacy in China is dead. Most importantly, through the examination of these three jurisdictions, there is strong evidence to suggest that these nation states are not so different when it comes to the invasion of Internet privacy. Despite these, there is still hope and the research concludes by examining possible ways to prevent the demise of Internet privacy.

Table of Contents

List of Tables

List of Figures

Table of Cases

Court of Justice of the European Union

United States

US v Truong 629 F.2d 908, United States of America, Appellee, v. Truong Ding Hung, Appellant. United States of America, Appellee, v. Ronald Louis Humphrey, Appellant.

US v Warshak 631 F.3d 266 (6th Cir. 2010)

Weiss v United States 308 US 321 (1939)

Whalen v Roe 429 US 589 (1977)

Warshak v United States 490 F.3d 455 (2007)

Warshak v United States 532 F.3d 521 (6th Cir. 2008)

United Kingdom

David Davis and others v Secretary of State for the Home Department [2015] EWHC 2092 (Admin)

Entick v Carrington, 19 Howell's State Trials 1029 (1765)

Harlan Laboratories UK Ltd & Anor v Stop Huntingdon Animal Cruelty ("SHAC") & Anor EWHC 3408 (QB) (7/12/12)

Investigatory Powers Tribunal [2014] UKIPTrib 13_77-H

Investigatory Powers Tribunal [2015] UKIPTrib 13_77-H

Malone v Commissioner for the Metropolitan Police (no.2) [1979] 344 Ch.

Media CAT Limited v Adams & Others [2011] EWPCC 6

Michael Douglas, Catherine Zeta-Jones, Northern & Shell plc v Hello! Limited, [2000] EWCA Civ 353

Prince Albert v Strange [1849] EWHC Ch J20 (8 Feb 1849)

R v Effick and Mitchell (1994) 99 Cr App Rep 312

Tolley v J.S. Fry & Sons Ltd [1930] 1 KB 467

Ireland

Table of Legislation

China

Computer Information Network and Internet Security, Protection and Management Regulations, approved by the State Council on December 11, 1997 and promulgated by the Ministry of Public Security on December 30, 1997

Constitution of the People's Republic of China

Criminal Law of the People's Republic of China as amended by Amendment 7 on February 28th, 2009

Explanations of a Number of Issues in the Specific Application of the Law on Handling Criminal Cases of Using the Internet, Mobile Communications Terminals, and Voice Sets for the Production, Reproduction, Publication, Sale, and Dissemination of Obscene Electronic Information, 6th September, 2004

General principles of the civil law of the People's Republic of China

Interim Provisions Governing the Management of the Computer Information Networks in the People's Republic of China Connecting to the International Network, adopted at the 42nd Executive Meeting of the State Council on January 23, 1996, promulgated by Decree No. 195 of the State Council of the People's Republic of China on February 1, 1996

Interim Provisions Governing the Management of the Computer Information Networks in the People's Republic of China Connecting to the International Network, promulgated by Decree No. 195 of the State Council of the People's Republic of China on February 1, 1996, and revised in accordance with the Decision of the State Council Regarding the Revision of the Interim Provisions Governing the Management of the Computer Information Networks in the People's Republic of China Connecting to the International Network, promulgated on May 20, 1997

Measures for the Management of Internet E-mail services

Council of Europe

Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols No. 11 and 14, 213 U.N.T.S. 222, signed on 4 November 1950, entered into force 3 September 1953; Protocol 14 was incorporated on 1st June 2010 (ECHR)

International Covenant on Civil and Political Rights (adopted 16 December 1966, entered into force 23 March 1976) 999 UNTS 171 (ICCPR)

International Covenant on Economic, Social and Cultural Rights (adopted 16 December 1966, entered into force 3 January 1976) 999 UNTS 3 (ICESCR)

United Nations

Universal Declaration of Human Rights (adopted 10 December 1948 UNGA Res 217 A(III)) (UDHR)

European Union

Charters

Charter of Fundamental Rights of the European Union, 2000/C 364/01, 18 December, 2000

Directives

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281

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 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks amending Directive 2002/58/EC

Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communication networks and services,

Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communication networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws

Regulations

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (GDPR)

United Kingdom

Acts of Parliament

Anti-terrorism, Crime and Security Act 2001

British Telecommunications Act 1981

Counter-Terrorism and Security Act 2015

Data Protection Act 1984

Data Protection Act 1998

Data Retention and Investigatory Powers Act 2014

Human Rights Act 1998

Interception of Communications Act 1985

Investigatory Powers Act 2016

Justices of the Peace Act 1361

Post Office Act 1969

Post Office (Protection) Act 1884

Regulation of Investigatory Powers Act 2000

Security Services Act 1989

Telecommunications Act 1984

Telegraph Act 1863

Telegraph Act 1868

Statutory Instruments

Data Retention (EC Directive) Regulations 2007, SI 2007/2199

Data Retention (EC Directive) Regulations 2009, SI 2009/859

Privacy and Electronic Communications (EC Directive) Regulations 2003, SI 2003/2426

Privacy and Electronic Communications (EC Directive) (Amendment) Regulations 2011, SI 2011/1208

Retention of Communications Data (Code of Practice) Order 2003, SI 2003/3175

Retention of Communications Data (Extension of Initial Period) Order 2003, SI 2003/3173

Retention of Communications Data (Further Extension of Initial Period) Order 2005, SI 2005/3335

Telecommunications (Data Protection and Privacy) Regulations 1999, SI 1999/2093

Telecommunications (Data Protection and Privacy) (Amendment) Regulations 2000, SI 2000/157

United States of America

Authorization for Use of Military Force, Pub L. 107-40, 115 Stat. 224, Sept 18, 2001

Communications Act of 1934, 47 USC S151 et seq.

Communications Assistance for Law Enforcement Act of 1994, Pub. L. No. 103-414, 108 Stat. 4279

Counterintelligence access to telephone toll and transactional records, 18 USC 2709 (2000 & Supp. I 2002)

Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848

Executive Order 11905, 41 Fed. Reg. 7703 (Feb 18, 1976)

Executive Order 12036, 43 Fed. Reg. 3674 (Jan 24, 1978)

Executive Order 12333, 46 Fed. Reg. 59941 (Dec 4, 1981)

Foreign Intelligence Surveillance Act of 1978 (Pub. L. 95–511, 92 Stat. 1783, 50 USC Ch. 36)

Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008, Pub. L. 110-261, 122 Stat. 2436, July 10, 2008

General prohibition on pen register and trap and trace device use; exception, 18 USC S3121

Intelligence Reform and Terrorism Protection Act of 2004, Pub. L. 108-458, 118 Stat. 3638, December 17, 2004

National Security Act of 1947, Chapter 343, 61 Stat. 496, July 26, 1947

New York State Consolidated Laws, Civil Rights, Sec 50 Right of privacy

Omnibus Crime Control and Safe Streets, Pub. L. No. 90-351, 82. Stat. 197

Privacy Act of 1974, Pub. L. 93–579, 88 Stat. 1896, December 31, 1974

Protect America Act of 2007, Pub. L. No. 110-55, Aug 5 2007, 121 Stat. 552

Stored Communications Act, 18 USC Ch. 121 S2701-2712

Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline Over Monitoring Act of 2015, Pub. L. 114-23, June 2 2015, 129 Stat. 268

Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001, PL 107-56, October 26, 2001

List of Abbreviations

9/11	The date (11th September, 2001) of the terrorist attacks against the World Trade Center and the Pentagon in the United States of America
ADSL	Asynchronous Digital Subscriber Line, typically used to connect the home and small business to the Internet. A component part of the generic Broadband
AES	Advanced Encryption Standard
AOL	America Online, Inc.
AS	Autonomous System
ASN	Autonomous System Number
AT&T	American Telephone & Telegraph; now branded AT&T
ATCSA	The Anti-terrorism, Crime and Security Act 2001
AUMF	The Authority for Use of Military Force
Broadband	Typically ASDL, broadband provides an always-on Internet connection to the home or small business. It is termed broadband as data travels to and from the home spread across a radio frequency spectrum carried on the telephone network
BT	British Telecommunications, Plc. Now branded BT
BULLRUN	Programme to defeat encryption
CA	Certificate Authority
CALEA	The Communications Assistance for Law Enforcement Act
CANET	China Academic Network
CCDP	The Communications Capabilities Development Programme
CDN	Content Delivery Network
CERNET	The China Education and Research Network
CG-NAT	Carrier Grade Network Address Translation
CIA	The Central Intelligence Agency

CJEU	Court of Justice of the European Union
CLS	Cable Landing Station. Connects subsea cables to country Internet
CNE	Computer Network Exploitation
CoE	The Council of Europe
CPC	The Chinese Communist Party
CSP	Communications Service Provider / Communications Service Providers. The term is wider than an ISP which only provides Internet services. Major telecoms companies such as BT are CSPs
CTSA	The Counter-Terrorism and Security Act 2015
DANE	The DNS-based Authentication of Named Entities
DHCP	Dynamic Host Control Protocol. A mechanism which can dynamically allocate IP addresses to attached devices. A typical home setup will use DHCP to allocate a private IP address to any attached device
DNA	Short for deoxyribonucleic acid
DNS	Domain Name System. A global distributed database which maps IP addresses to system names, for example 129.11.26.33 is www.leeds.ac.uk
DNSSEC	DNS Security Extensions
DPA	The Data Protection Act 1998
DPA84	The Data Protection Act 1984
DPI	Deep Packet Inspection. The technique of looking into data packets to reveal information contained within the payload
DPRIVE	DNS PRIVate Exchange
DRD	The Data Retention Directive
DRIPA	The Data Retention and Investigatory Powers Act, 2014
Dual_EC_DRBG	The Dual Elliptic Curve Deterministic Random Bit Generator
E2EE	End-to-End Encryption
ECHR	The European Convention on Human Rights

ECPA	The Electronic Communications Privacy Act of 1986
ECtHR	The European Court of Human Rights
EC	The European Commission
EES	The Escrowed Encryption Standard
E-mail	Electronic Mail
EPIC	The Electronic Privacy Information Center
Ethernet	A commonly used physical network
FAA	The FISA Amendments Act of 2008
FBI	Federal Bureau of Investigation
FISA	The Foreign Intelligence Surveillance Act of 1978
FISC	The Foreign Intelligence Surveillance Court
FISCR	The United States Foreign Intelligence Surveillance Court of Review
Five Eyes	Five Eyes is a group of countries which share intelligence and consist of: Australia, Canada, the UK, the US and New Zealand
FoxAcid	Programme to de-anonymise Tor users
GCHQ	The UK Government Communications Headquarters
GDPR	The General Data Protection Regulation
HRA	The Human Rights Act 1998
HTTP	Hypertext Transfer Protocol
IAP	Internet Access Providers
ICCPR	The International Covenant on Civil and Political Rights
ICESCR	The International Covenant on Economic, Social and Cultural Rights
ICP	Internet Content Provider
ICR	Internet Connection Record
IETF	Internet Engineering Task Force
IHEP	The Institute of High Energy Physics

IMP	The Intercept Modernisation Programme
Internet	Global network formed out of the interconnection of many networks and using common protocols
IOCA	The Interception of Communications Act 1985
IoT	The Internet of Things
IP	Internet Protocol
IPv4	IP version 4, which is current
IPv6	IP version 6, next generation, being implemented
IPT	Investigatory Powers Tribunal
ISC	The Intelligence and Security Committee
ISP	Internet Service Provider. This may be an access provider, or a provider of services such as web hosting, or a combination
IXP	Internet eXchange Point
M2M	Machine to Machine communication
MAC	Media Access Control
MEI	The Ministry of Electricity Industry
Metadata	Communications data, data about a communication but not including content
MITM	Man In The Middle attack
MOTS	Man On The Side attack
MP	Member of Parliament
MPT	The Ministry of Posts and Telecommunications
NAACP	The National Association for the Advancement of Colored People
NAT	Network Address Translation
NIST	The National Institute of Standards and Technology
NPC	The National People’s Congress
NSA	The National Security Agency

NSL	The National Security Letter
OCCSSA	Omnibus Crime Control and Safe Streets Act
OSI	Open Systems Interconnection
OSX	Macintosh Operating System X
OTA	The Office of Technology Assessment
PAA	The Protect America Act of 2007
PCLOB	The Privacy and Civil Liberties Oversight Board
PECR	The Privacy and Electronic Communications (EC Directive) Regulations 2003
Pen Register	A device which logs all number dialled by a phone being monitored. In modern terms, such a device would monitor all IP addresses connected to by a system being monitored
PET	Privacy Enhancing Technology
PGP	Pretty Good Privacy – encryption software
PKI	Public Key Infrastructure
PRISM	US mass Internet collection programme
PSB	The Public Security Bureau
PSP	The President's Surveillance Program
RFID	Radio-Frequency IDentification
RIPA	The Regulation of Investigatory Powers Act 2000
RSA	RSA has multiple related meanings. RSA is formed from the initials of Ron Rivest, Adi Shamir and Leonard Adelman who pioneered public key cryptography; as a company, RSA Security produce cryptographic libraries
Router	A device which interconnects network segments and determines what data needs to go where by examining the destination IP address
RUSI	The Royal United Services Institute
SCA	The Stored Communications Act
SLAC	Stanford Linear Accelerator Center

SMS	Short Message Service
SNI	Server Name Indication
SPI	Shallow Packet Inspection
TCP	Transmission Control Protocol (as in TCP/IP)
Tempora	UK mass Internet collection programme
Tor	‘The Onion Router”
traceroute	A command which uses Internet control packets to estimate the route those packets are taking
Trap and Trace Device	A device which records all numbers calling the monitored phone. In modern terms, this would record all IP addresses connecting to a monitored system
TSP	The Terrorist Surveillance Program
UDHR	The Universal Declaration of Human Rights
UDP	User Datagram Protocol
Upstream	US mass Internet collection programme
URL	Uniform Resource Locator, a web address
USC	United States Code
VoIP	Voice over Internet Protocol
Web	Short for World Wide Web
Web2.0	The second generation Web
whois	A database containing registrant information for Internet domain names
Wi-Fi	Wi-Fi is the name adopted by the Wi-Fi Alliance to describe the common Wireless LAN (WLAN) technology working to IEEE Standard 802.11
VoIP	Voice over IP
VPN	Virtual Private Network

Chapter 1: Introduction

1.1 Background

In 2016, it was reported that the Internet is used by almost half the population of the world.[1] Electronic mail (E-mail) allows us to communicate without the need to write and then post a physical letter. The invention of the World Wide Web (Web)[2] enabled people to access and use resources scattered about the Internet. We have come to rely on it for personal banking, business and personal communications, news, television and entertainment. The Web also gave rise to social media websites such as Facebook.[3] Social media websites allow us to connect with people and form groups, or just to tell everyone what we are doing or how we feel. The mobile phone became the smartphone, a device which retains the utility of a telephone while being a mobile communications device capable of a wide variety of tasks, which allows us to be connected all the time and wherever we are. We are increasingly living our lives in public.

However, because of its nature, the Internet is also a rich ground for those who wish to surveil an individual and/or a population. Communications technologies have always been subjected to targeted surveillance, for example, a telephone tap. The Internet enables mass surveillance, where

---

[1] International Telecommunications Union, 'ICT Facts and Figures 2016' <https://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2016.pdf> accessed 26 December 2016

[2] The World Wide Web was invented at CERN by Tim Berners-Lee in 1989. See <http://webfoundation.org/about/vision/history-of-the-web/> accessed 16 October 2016

[3] Facebook is a popular social media site. Founded in 2004 it reportedly had 1.79 billion active users as of 30 September 2016; see <http://newsroom.fb.com/company-info/> accessed 13 November 2016

information being shared not just between targeted individuals, but also between all people can be acquired.

Today, the Internet has over 3.4 billion users.[4] In 2015, there were 59.3 million Internet users in the UK (64.7 million population),[5] 280.7 million in the US (321.3 million population),[6] and 721.4 million Internet users in the People's Republic of China (China) (1.37 billion population).[7] As can be seen from these statistics, China has more Internet users than the number of *people* in the UK and US combined.[8]

Unlike the US and the UK, the ease of access to news and information presented an issue for China. Since the Internet began in China, the government has sought to control it, primarily because the Internet offers information that may lead to social instability. If the Chinese government is to maintain control it needs to keep a grip on the flow of information into China.

---

[4] International Telecommunications Union, 'Key ICT indicators for developed and developing countries and the world (totals and penetration rates)' <http://www.itu.int/en/ITU-D/Statistics/Documents/statistics/2016/ITU_Key_2005-2016_ICT_data.xls> accessed 26 December 2012

[5] Miniwatts Marketing Group, 'Internet in Europe Stats' <http://www.internetworldstats.com/stats4.htm#europe> accessed 1 October 2016

[6] Miniwatts Marketing Group, 'Internet Usage and 2015 Population in North America' <http://www.internetworldstats.com/stats14.htm#north> accessed 1 October 2016

[7] Miniwatts Marketing Group, 'Internet Usage in Asia' <http://www.internetworldstats.com/stats3.htm#asia> accessed 1 October 2016. Note these figures do not include Hong Kong (5.7 million Internet users, 7.1 million population)

[8] The Office for National Statistics in the UK estimated there were 56.1 million people resident in the UK on 27 March 2011, see <http://www.ons.gov.uk/ons/rel/census/2011-census/key-statistics-for-local-authorities-in-england-and-wales/stb-2011-census-key-statistics-for-england-and-wales.html> accessed 24 March 2013. The US Census Bureau projection for 30/06/15 was over 316 million, see <http://www.census.gov/population/www/popclockus.html> accessed 27 December 2012.

China has the benefit of owning the Communications Service Providers (CSPs) responsible for international connections and was able to build a sophisticated firewall to control the flow of information. Additionally, there is an army of censors who can watch what people are accessing and it gives China the level of control it desires.[9]

The Chinese level of control is at odds with the apparent freedom offered in the US and the UK. However, the Internet has changed privacy. Where one might talk quietly to someone, one now uses e-mail or messengers. When talking face to face, you are able to avoid being overheard, perhaps, by standing in a secluded area. When using the Internet, one may feel the same level of privacy but in reality, one's communication is mixed with everyone else's and transmitted across common cables. Where surveillance is concerned, this is more like shouting your conversation across a crowded room.

In the post-9/11[10] world, terrorism is seen as a very real threat to society and the Internet is seen as a mechanism that enables terrorists to spread their ideology, to raise funds, and to communicate plans. It is this which is the driver of new and often secret programmes, Internet laws and regulations in the US and the UK. Whereas China uses its desire to control the population as a reason to control the Internet, the US and UK see the openness and freedom of the Internet as an enabler of crime and terrorism.

The Snowden revelations of 2013 showed the world exactly how far nation states can and will go in order to mount mass surveillance operations to gather Internet communications. These revelations are ongoing but have already indicated that the US Government allegedly taps into social media providers, and the US and UK Governments tap into oceanic cables which interconnect

---

[9] Electronic Privacy Information Center, *Privacy & Human Rights: an international survey of privacy laws and developments* (Electronic Privacy Information Center, 2003), 205

[10] 11 September, 2001 was the date of the terrorist attack on the twin towers of the US World Trade Center and Pentagon. It became known as '9/11'.

countries and continents in order to extract and analyse all data flowing across them.

The structure of the Internet makes it the ideal surveillance platform. If data can be read in transit and if the sender and recipient of messages can be discovered, then no-one is safe from the prying eye of the State. The fact that our mobile devices allow us to live our lives in public is a great aid to the States' desire to surveil its populous.

From the above, it has shown the relationship between Internet privacy, Internet technologies and surveillance legislations are complex. Hence, this research aims to increase the understanding of the effects of surveillance legislation versus technological possibilities governed by the functioning of the Internet in order to address a frequently asked question 'is Internet privacy dead?'.

1.2 Research scope, aim and objectives

Surveillance has always been with us. Any form of census is a form of surveillance. On one hand, surveillance has benefits for society from the detection and prevention of crime to the detection and early diagnosis of disease.[11] For instance, systems and processes which check on our health are clear benefits. On the other hand, surveillance can have a chilling effect on our lives, especially if we are members of certain groups.[12] Taken to extreme it can prevent us from pursuing the freedoms we have become accustomed to**.**

---

[11] See for example J S Brownstein and others, 'Surveillance Sans Frontières: Internet-Based Emerging Infectious Disease Intelligence and the HealthMap Project' <http://www.plosmedicine.org/article/info:doi/10.1371/journal.pmed.0050151> accessed 19 January 2011

[12] Dawinder S Sidhu, 'The chilling effect of government surveillance programs on the use of the Internet by Muslim-Americans' [2007] 7 U Maryland Journal of Race, Religion, Gender and Class, 375

It would seem that some level of surveillance is essential in our society. However, responses to new threats may become increasingly invasive. Fighting against terrorism and serious crime are often used to justify the erosion of privacy in general and increasingly Internet privacy.

Surveillance on the Internet is a new battleground which attracts much attention from all walks of life in our society. Since the 2013 Snowden revelations, the practice of Internet surveillance has become common knowledge.

Nevertheless, there is a lack of existing literature directly addressing the following questions

1. Is Internet privacy dead?
2. Have the US and the UK reached the level of China with regard to the invasion of Internet privacy?
3. What measures can be taken to prevent mass Internet surveillance from destroying Internet privacy?

Hence, the above become the research questions of this research and the aim is to fill these intellectual gaps.

This research aims to examine the extent to which Internet privacy is preserved or violated via an examination of a set of jurisdictions; namely, the US, UK and China. In this research the focus is specifically geared to the technical aspect of the Internet in order to express how technology is used to enhance and invade privacy. The rationales of choosing these three jurisdictions for use in this research are given in the next section.

To achieve the research aim, a set of research objectives were set out and they are depicted as follows.

1. Analyse the meaning of privacy generally, and Internet privacy specifically
2. Examine the development of communications surveillance and legislation in the three chosen jurisdictions

3. Examine the technical measures which both enhance and invade Internet privacy, in particular in the light of the 2013 Snowden revelations
4. Evaluate the fate of Internet privacy and provide recommendations

It is important to note that the scope of this research is confined to Internet privacy with regard to surveillance as opposed to surveillance in the wider sense.

1.3 Justification of the chosen jurisdictions

In 2007, Privacy International and the Electronic Privacy Information Center (EPIC) published a world map of surveillance societies. In this, eight jurisdictions were listed as having endemic surveillance. These were China, Malaysia, Russia, Singapore, Taiwan, Thailand, the US and the UK.[13] After the 2013 Snowden revelations the US and the UK were shown to be engaged in mass Internet surveillance on a global scale.

Three jurisdictions have been chosen for use in this research and they are: the US, the UK and China.

US

The US - the 'land of the free'[14] - is chosen as it has some level of constitutional protection, and has developed privacy protection further than the UK.

The US has, however, introduced a number of laws explicitly allowing its agencies to spy on its population and, moreover, to spy on anyone else it

---

[13] Zetter, K., 'World's Top Surveillance Societies' <https://www.wired.com/2007/12/worlds-top-surv/> accessed 8 January 2017)

[14] The Star Spangled Banner <http://www.loc.gov/exhibits/treasures/images/uc05112x.jpg> accessed 24 January 2009

wants. The Foreign Intelligence Surveillance Act (FISA)[15] was originally put into place to govern surveillance of foreign powers and agents but it has been modified in the wake of 9/11 by the USA PATRIOT Act[16] to more specifically deal with terrorism anywhere. The Communications Assistance for Law Enforcement Act (CALEA)[17] ensures the US Government has access to telecommunications networks for surveillance purposes. Over many years, evidence has come to light of the US Governments 'illegal wiretapping' activities, from the Federal Bureau of Investigation (FBI)'s Carnivore[18] project to AT&T's 'room 641A'.[19] The US Government's reaction has been to attempt to enact laws to legitimise such actions.

UK

The UK is chosen because it has not developed any actual privacy laws, favouring extending existing laws instead. The UK has enacted a number of privacy-invasive laws since before 9/11 and has been criticised by the European Court of Human Rights (ECtHR)**.** The Human Rights Act 1998 gave further effect to the European Convention on Human Rights (ECHR)[20] within UK law. In addition to the ECtHR decisions, these have resulted in the Regulation of Investigatory Powers Act 2000 (RIPA).

---

[15] Pub. L. No. 95-511, 92 Stat. 1783, enacted 25 Oct 1978, 50 UCS Ch. 36.

[16] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, Pub. L. No. 107-56

[17] Communications Assistance for Law Enforcement Act of 1994 (Pub. L. No. 103-414, 108 Stat. 4279), codified at 47 USC 1001-1010

[18] Carnivore was an Internet packet sniffer capable of recording Internet traffic for analysis.

[19] AT&T's Room 641A is a room where, allegedly, major Internet links were paired so that all traffic passing along them could be recorded and fed to the NSA

[20] Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols No. 11 and 14, 213 U.N.T.S. 222, signed on 4 November 1950, entered into force 3 September 1953; Protocol 14 was incorporated on 1st June 2010 (ECHR)

While purporting to rationalise surveillance and subject it to the courts, RIPA also opened up surveillance to a large number of agencies. As a result of this, it has been used to permit surveillance of minor infringements such as dog fouling[21] and domestic waste infringements; while these are likely to be disproportionate, it may well be beneficial to report on dog fouling in children's playgrounds due to health risks[22]. Terrorism legislation has been used to freeze non-terrorism related assets during the credit crunch[23]. Examples such as these must push the test 'necessary in a democratic society'[24] to the limit. It is also clear that the ECtHR will readily criticise UK laws; for example, with it finding against the UK plans to store DNA data,[25] and finding that the power to stop and search vehicles and people granted under s.44 of the Terrorism Act 2000 is not in accordance with the law and therefore violates ECHR Art.8.[26]

China

Unlike the US and the UK, China is historically not a democratic regime. Historically, the social unit in China was the family, not the individual,[27] the

---

[21] 'Spy law used in dog fouling war' (*BBC News*, 27 April 2008) <http://news.bbc.co.uk/1/hi/uk/7369543.stm> accessed 19 January 2011

[22] Office of the Surveillance Commissioners Annual Report for 2009-2010, s5.20

[23] The Landsbanki Freezing Order 2008 (SI2008/2668) was created under s.10(2) of the Anti-terrorism, Crime and Security Act 2001 in order to deal with the effects on the UK of the collapse of the Icelandic bank.

[24] ECHR (n 20) Art 8(2)

[25] *S. and Marper v. The United Kingdom*, Application nos. 30562/04 and 30566/04 (ECtHR, 4 December 2008)

[26] *Gillan and Quinton v. the United Kingdom*, Application no. 4158/05 (ECtHR, 12 January 2010)

[27] Edward Williams, *China yesterday and to-day* (5th edn. Revised) (Harrap, London, 1932) p54

family having no privacy away from each other.[28] China's laws were biased towards duty and against rights.[29] The concept of a ‘private realm free from external interference’[30] does not fall within Chinese culture of old and remains ‘underdeveloped’.[31] The concept of freedom in China was generally taken to be freedom to serve the state and society, with the needs of the collective always put before the needs of the individual,[32] this collectivism that making it impossible to consider individual rights.[33] Unlike the Western liberal view that the individual is an autonomous component and society only a group of individuals voluntarily committed to cooperate together for a common goal, the Chinese view is that individuals are born into families within a society, and are not autonomous, being bound to their communities.[34]

China is thus chosen to give an opposing view to those of the US ad UK. Furthermore, China is chosen in this research because of its efforts to control the flow of information into the country via the Internet. It has established a system of firewalls and human operatives who monitor Internet access and content.

---

[28] Shin-Yi Peng, ‘Privacy and the construction of legal meaning in Taiwan’, 37 Int’l L. 1037 2003, p1039

[29] Jingchun Cao, 'Protecting the right to privacy in China', 36 Victoria U. Wellington L. Rev. 645 at 646

[30] Edmund S K Fung, 'The idea of freedom in modern China revisited: plural conceptions and dual responsibilities', Modern China, Vol. 32, No. 4 (Oct 2006) 453 at 468

[31] Ibid., 470

[32] Ibid., 454

[33] Guo Liang and Chang Huili, Surveillance and privacy in urban China, the Globalization of Personal Data project, Queen's University, 2006, p1

[34] George F Ling, *China developing: cultural identity of emerging societies* (World Scientific, Singapore, 2008), 21

1.4 Research methodology

This research uses a doctrinal method in order to achieve the research aim and objectives and address the research questions. The doctrinal method used draws from a wide range of sources across the three selected jurisdictions, namely the US, the UK and China. It examines primary sources from each jurisdiction in the form of cases, legislation and treaties, as well as supranational and regional cases and legislation specifically regarding the UK. Additionally, a wide range of secondary sources including journal papers and books have been examined. The doctrinal method is 'rarely discussed'[35] in methodology sections of research publications and such a statement would seem out of place in a doctrinal thesis.[36] Nevertheless, a brief explanation of the method and why it is relevant to this research cannot be ignored.

Doctrinal research, also known as library-based or theoretical research is the most common methodology used by researchers in the field of law.[37] Using the method the researcher compiles and then analyses primary sources, for example case law and relevant legislation and regulations, and secondary sources such as journals. This is often done from a historical perspective and the primary aim is to describe the law and how it applies to the research topics.[38] The methodology is a qualitative form of legal research which allows the legal researcher to choose both depth and breadth of study.[39] The reason for using doctrinal methodology in this research is because it fits the need to determine what laws have enabled surveillance from a historic perspective as

---

[35] Terry Hutchinson and Nigel Duncan, 'Defining and Describing What We Do: Doctrinal Legal Research', 17 Deakin L. Rev. 83 (2012), 100

[36] Ibid.

[37] Ashish Kumar Singhal and Ikramuddin Malik, 'Doctrinal and socio-legal methods of research: merits and demerits', 2(7) Educational Research Journal 252-256, 2012, 252

[38] Ian Dobinson and Francis Johns, 'Qualitative Legal Research' in Mike McConville and Wing Hong Chiu (Eds.) *Research Methods for Law* (Edinburgh University Press, Edinburgh, 2007), 19

[39] Hutchinson and Duncan (n 35) 107

well as analyse the effect of these on Internet privacy. The research analyses the legal rules in the three jurisdictions in order to investigate the research questions. The focus is on laws from early communications surveillance, for example telephone tapping, up to the interception of Internet communications in order to determine how laws have been shaped through time.

The research also adopts a descriptive method in parts, in particular when discussing the technology of the Internet and technical methods of invading and maintaining Internet privacy. This is necessary in order to provide an understanding of the Internet from a technical perspective in order to illustrate the risks to privacy from mass Internet surveillance.

It is also important to note that legislation and case law used in this research is correct up to 31 December, 2016.

1.5 Research limitations

The primary limitations in this research of China are the language barrier and access to materials. Publications tend to add no new information of relevance to this research.[40] Official translations of legislation are not regularly updated, and unofficial translations often contradict each other and so cannot be used.

In addition to this, China has a relatively new legal system dating from 1978 after the end of the Mao era. What literature exists which may be of use is generally written by Western academics based outside China and while much has been written there is little specific to this research other than those quoted in Chapter 5.

Additionally, it is extremely difficult to tap into the Chinese networks. It requires a substantial time to get to know the 'right' people who can provide sources of information required by this research. Even then, and being

---

[40] Examples include: Hao Wang, *Protecting Privacy in China: A Research on China's Privacy Standards and the Possibility of Establishing the Right of Privacy and the Information Privacy Protection Legislation in Modern China* (Springer, Berlin, 2011); Guosong Shao, *Internet law in China* (Chandos, Oxford, 2012)

introduced via Chinese friends, when academics found that the research was about human rights and privacy they refused to help and communication ground to a halt.

Furthermore, challenging personal circumstances have emerged during the course of the research which caused an interruption to the research and lengthened the time for completion.

1.6 Structure of the thesis

This thesis is presented in seven chapters including this introductory chapter.

Chapter 2 investigates the meaning of privacy in general and focuses on privacy as an enabler of autonomy and liberty. Focus then moves to an examination of sources of privacy in the three chosen jurisdictions. It then examines the Internet from a technical perspective in order to provide an understanding of the risks posed to privacy by technology.

Chapter 3 investigates the development of communications surveillance in the US using an analysis of key cases. It examines key legislation.

Chapter 4 investigates the development of data protection in the UK as this is considerably different from the limited protection in the US. Focus then moves to an analysis of communications surveillance in the UK using key cases and examination of key legislation.

Chapter 5 investigates the development of the Internet in China and the desire to control the flow of information into China. It examines key legislation which affects the Internet.

Chapter 6 provides a much greater technical analysis of the functioning of the Internet in order to then examine the issues surfaced by the 2013 Snowden revelations.

Chapter 7 provides potential solutions along with an answer to the research questions.

Chapter 2: Privacy and the Internet

2.1 Introduction

In order to understand Internet privacy and how this may be lost or protected, it is first necessary to examine the two key elements: privacy; and the Internet.

The word 'privacy' is simple in that it is a widely recognised concept. Everyone has something they would not wish to be made public, perhaps simply details of intimacy that has no place in the public domain. Feldman states that privacy is a ‘necessary condition for human flourishing’.[41] Westin takes this a step further, indicating that even in the animal kingdom the desire for ‘individual seclusion or small-group intimacy’[42] exists. Although Mead’s study of the Samoan people found little recognisable privacy, for example there being no privacy within houses and it being common for all the members of a village to know about all the actions of every other village member,[43] even here there is a sense of what should be private, with public signs of affection being considered shameful and commenting on sex or evacuation in public not being good taste.[44]

However, although it can be argued that awareness of privacy is universal regardless of one’s ability to say the word,[45] even a simple definition of the word is problematic. According to the Oxford English Dictionary, privacy can mean ‘to seclude’[46] or refer to something which is ‘[r]estricted to one person

---

[41] David Feldman, *Civil liberties and human rights in England and Wales*, (2nd edn) (OUP, Oxford, 2002), 512

[42] Alan Westin, *Privacy and Freedom* (Athenum, New York, 1970), 8

[43] Margaret Mead, Coming of Age in Samoa (Penguin, Middlesex, 1943), 104

[44] Ibid., 112-113

[45] Bonnie S McDougall, 'Particulars and universals: studies on Chinese privacy' in Bonnie McDougal and Anders Hansson (eds) *Chinese Concepts of privacy* (Brill, The Netherlands, 2002), 7

[46] OED Online available online via the University of Leeds Library

or a few persons as opposed to the wider community'.[47] It can mean a place 'unfrequented [or] secluded',[48] or a person 'retiring, reclusive; ... reserved, unsociable',[49] or, perhaps a couple 'undisturbed by others'.[50] The Webster's Third New International Dictionary defines privacy as 'being apart from the company or observation of others',[51] while the Oxford American Dictionary of Current English defines it as 'the state of being private and undisturbed',[52] or, simply the 'right to be left alone'.[53] In Chinese, privacy (yǐnsī - 隱私) is made up of two words, 隱 (yǐn) meaning to hide, and 私(sī) meaning private.[54] It was common for the Chinese people to interpret privacy as being a 'shameful secret'[55] or an indication of selfishness, secrecy and underhandedness[56] as well as a 'state of seclusion'.[57]

Privacy as a concept may be easy to understand. Closing a door to have a conversation while not being overheard by others indicates one's desire for privacy. However, privacy has bounds and it is important to understand where and how one may expect privacy, and where one may not.

Privacy can be given away, intentionally or otherwise. For example, two people arguing and shouting at each other in a room with the windows open

---

[47] Ibid.

[48] Ibid.

[49] Ibid.

[50] Ibid.

[51] Webster's Third New International Dictionary of the English Language (Bell, 1961)

[52] Oxford American Dictionary of Current English (OUP, Oxford, 1999)

[53] Oxford Dictionary of Law, (OUP, Oxford, 2006, 6th edn)

[54] Cao (n 29), 646

[55] Ibid.

[56] McDougall (n 45) p6

[57] Ibid.

and thus easily heard from the street may still have an expectation of privacy; for example they may not expect their argument to appear in the newspapers, but they are making it hard for their privacy to be maintained.[58]

Privacy can be invaded as it can be taken from us. Invasion of privacy is a one-way street. If private information is published or heard, it cannot be *un*-published or *un*-heard. Once made public, 'private information cannot be made private again'.[59] This is particularly true on the Internet where information can easily be copied or re-purposed by just about anyone; the effect being that, unlike a magazine where technically one could stop production and acquire any distributed copies, once on the Internet, information has a tendency to spread, either posted verbatim for example on numerous blogs, or modified and posted out of context. It is then impossible to control or retract.

The Internet complicates the concept of a private space. Communicating over the Internet may give an appearance of privacy in that only two people may be communicating. However, the Internet is a complex technology which makes the communications path between people appear simple. There is a danger in ignoring, or simply being ignorant, of the fact that one's Internet communications traverse the Internet via service providers, each of which technically has access to the communications path and everything passing across it. Therefore, in order to discuss Internet privacy one must understand the basics of how the Internet itself functions.

The aim of this chapter is to examine the meaning of the word privacy and set it in an Internet context (Section 2.2). The objectives are to show how privacy is defined in International law as well as in each of the three selected jurisdictions, and then look more specifically at Internet privacy both from a technical perspective (Section 2.3) and also in daily life (Sections 2.4 and 2.5).

---

[58] Judith Jarvis Thompson, 'The Right to Privacy', Philosophy and Public Affairs, Vol 4, No 4 (Summer, 1975), p296

[59] Doug D Tygar, 'Technological dimensions of privacy in Asia', 10 Asia-Pacific Review 2, 124

This is because it is necessary to understand the technology behind the Internet in order to understand the risks it poses to one's Internet privacy. The Internet is very different from a simple telephone line connecting two people. It consists of a plethora of interconnected technologies and communications protocols which both ensure that communications are possible but also provide an ease of interception of communications. Most importantly, these are typically not understood well by law and policy makers.

2.2 Privacy defined

Privacy has roots in both ancient Chinese and Greek philosophy. Wang suggests that the sayings of Confucius include an indication that one should not 'invade other people's private lives'.[60] Cao agrees, considering that Confucian philosophy includes the prohibition of 'invasion of a person's private life'[61] and in particular the disclosure of 'intimate relationships'.[62] Moore finds that Aristotle recognised the distinction between public and private spheres, specifically as the difference between the state and the household, life not necessarily being 'tied to public activity'.[63]

Privacy was defined by Cooley as simply the right 'to be let alone'.[64] Warren and Brandeis used this as the starting point to their article in the Harvard Law Review in 1890.[65] However, this right 'to be let alone' is extremely broad and

---

[60] Hao Wang, *Protecting privacy in China: a research on China's privacy standards and the possibility of establishing the right to privacy and the information privacy protection legislation in modern China* (Springer, Heidelberg, 2011), 36

[61] Cao (n 29) 647

[62] Ibid.

[63] Adam D. Moore, 'Privacy' in Hugh LaFollette (ed.) *International Encyclopedia of Ethics* (Wiley, Chichester, 2013), 4100

[64] Thomas Cooley, *A treatise on the law of torts or the wrongs which arise independent of contract* (Callaghan and Co., Chicago, 1880), 29

[65] Samuel D Warren and Louis D Brandies, 'The Right to Privacy' 4 Harv. L. Rev. 193

all encompassing. If privacy is simply this, then the concept is too broad to be the basis of a legal rule. That is to say pretty much any action of any kind against a person would not let him alone.

Of the influential writers on the subject, Westin approaches privacy from practical realities. He defines privacy as:

> the voluntary and temporary withdrawal of a person from the general society through physical or psychological means, either in a state of solitude or small-group intimacy or, when among larger groups, in a condition of anonymity or reserve.[66]

This withdrawal has the effect of giving a person or group of people the freedom to determine what information about themselves they share, and with whom and when they share it.[67] However, privacy is never absolute due to the needs of the individual to participate in society. The individual 'balances'[68] privacy and disclosure in the face of the 'curiosity of others'[69] and the 'processes of surveillance that every society sets in order to enforce its social norms.'[70] In fact, privacy encompasses a number of values including anonymity,[71] autonomy,[72] liberty, intimacy,[73] dignity,[74] solitude[75] and the control of personal information.[76] Kupfer states that privacy is 'a necessary

---

[66] Westin (n 42) 7

[67] Ibid.

[68] Ibid.

[69] Ibid.

[70] Ibid.

[71] Ibid., 31

[72] Ibid., 33

[73] Ibid., 31

[74] David Feldman, 'Human dignity as a legal value: part 1', [1999] Public Law 682

[75] Westin (n 42) 31

[76] Raymond Wacks, 'The Poverty of Privacy' (1980) 96 LQR 73

condition for something of basic value – the development of an autonomous self.'[77] By enabling personal autonomy, the 'bedrock value'[78] of classical liberalism, privacy can enable freedom of choice and promotes our very individuality.[79] Kupfer continues that privacy aids the formation of individual autonomy by allowing people to decide 'whether or not their physical and psychological existence becomes part of another's experience'[80] and gives us the 'choice and control over [the] disclosure of information'[81] about ourselves. Wacks states that removing a person's autonomy removes their freedom to choose to be private.[82]

Having the autonomy to make independent choices leads to trust.[83] Where an individual or group is not subjected to the 'meddling of outsiders',[84] they can make choices without external interference.[85] Additionally, being able to decide when to disseminate personal information increases our feeling that we are autonomous.[86] Where an individual is left to make choices, with the opportunity to make mistakes or do wrong, the responsible individual gains

---

[77] Joseph Kupfer, 'Privacy, autonomy and self-concept', 24 American Philosophical Quarterly 1 (Jan 1987) 81-89, 81

[78] Jack Hirshleifer, 'Privacy: its origin, function, and future', 9 J Legal Studies 4 649-664 (Dec 1980), 650

[79] Westin (n 42) 34

[80] Kupfer (n 77) 82

[81] Ibid., 85

[82] Wacks (n 76) 79

[83] Kupfer (n 77) 84

[84] Feldman, *Civil liberties and human rights in England and Wales* (n 41) 511

[85] Ibid.

[86] Westin (n 42) 34

the trust of society.[87] Equally, a loss of privacy threatens the individual's 'sense of trustworthiness'.[88]

Privacy is also a 'major contribution to an individual's dignity'.[89] In some cases, a lack of privacy has a detrimental effect on one's dignity; for example, when one's efforts in the gym are recorded and made public for the amusement of others.[90] It is also instrumental to liberty which is a fundamental value of the US Constitution. It can be difficult for a person to exercise the various freedoms that form liberty if there is no respect of a person's privacy. For example, religious freedom requires privacy for prayer. Freedom of association can be hard under scrutiny. Privacy is a 'precondition to freedom of expression';[91] for example, by enabling people to consult and draft items before publication.

According to Westin, solitude is the 'most complete state of privacy'[92] one can achieve. It can be defined as the state where an individual is separated from and not observed by anyone. In a state of solitude, privacy can also include the 'absence of … disturbing noises'.[93] Thus, if someone answers the phone only to hear a recorded message advertising some product no information is lost; however, the person may consider it an invasion of their privacy.[94]

---

[87] Kupfer (n 77) 84

[88] Ibid., 85

[89] Feldman, 'Human dignity as a legal value: part 1' (n 74) 685

[90] Ibid., 694

[91] Paul Chadwick, 'The value of privacy', EHRLR 2006, 5, 495-508, at 498

[92] Westin (n 42) 31

[93] William A Parent, 'Recent work on the concept of privacy', 20 American Philosophical Quarterly 4, 347

[94] Hirshleifer (n 78) 650

However, solitude could be compared to ‘alienation, loneliness, ostracism, and isolation’.[95] All are conditions of being alone. However, whereas privacy is sought, the other conditions may be feared.[96] One may want to be private but may not wish to be lonely. Furthermore, solitude cannot be considered a core value of privacy. It is not the norm as people tend to live together in communities of all sizes. A community would not work if all its people were completely isolated from one another and did not share information with others. To some greater or lesser extent, we all ‘lead lives exposed to the public gaze or to public inquiry’[97] as we exist in a society with others.

Having the autonomy to determine what information is known about us by a small group (e.g. spouse, family or friends) enables intimacy. Intimacy is created in part by ‘giving away some of our privacy freely to those we regard as close to us.’[98] Privacy thus becomes shared. However, we still exercise control over our personal information – we ‘reveal and share of ourselves as *we* choose’.[99] Intimacy is crucial to the ‘basic need of human contact’,[100] and without privacy, intimacy cannot be achieved.

Anonymity can be described as the ability of a person to find ‘freedom from identification and surveillance’[101] in the public arena. It is to be ‘unnamed,

---

[95] Michael A Weinstein, 'The uses of privacy in good life', in J Roland Pennock and John W Chapman (eds) *Privacy: Nomos XIII* (Atherton, New York, 1971), 88

[96] Ibid.

[97] William L Prosser, 'Privacy' 48 Cal. L. Rev 383 (1960), p396

[98] Chadwick (n 91) 497

[99] Ibid.

[100] Westin (n 42) 31

[101] Ibid.

unnoticed, part of a crowd.'[102] Westin finds that a 'major aspect of privacy for individuals … is the ability to move about anonymously from time to time'.[103]

As demonstrated from above, an invasion or loss of privacy not only results in the difficulty of a person to enjoy an area protected by privacy but also results in some piece of information about a person being known to others. This information might be the person's location, their (dis-)likes, who they are corresponding with, or who they are in a relationship with. Westin defines informational privacy as:

> the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others.[104]

Wacks identifies three problematic areas of privacy, namely: activities which 'intrude, physically or electronically, into home of office',[105] 'publicity given to'[106] and 'potential misuse of "personal information" '.[107] Therefore, rather than a wide protection of privacy, Wacks proposes the term 'protection of "personal information" '[108] with personal information being defined as:

> facts, communications or opinions which relate to the individual and which it would be reasonable to expect him to regard as intimate or confidential and therefore to want to withhold or at least to restrict their circulation.[109]

Here, Wacks defines what personal information is and Westin defines how it should be controlled. Informational privacy is discussed further below.

---

[102] David Brin, *The transparent society* (Basic Books, New York, 1998), 78

[103] Westin (n 42) 69

[104] Ibid., 7

[105] Wacks (n 76) 88

[106] Ibid.

[107] Ibid.

[108] Ibid.

[109] Ibid.

However, it is first necessary to determine what protections for privacy exist at an international and, in particular in the case of the UK at a regional level.

2.2.1 Privacy and international human rights

Internationally, human rights laws with specific protections of privacy were not formed until after WWII. Rights are defined in three key articles: the Universal Declaration of Human Rights (UDHR);[110] the International Covenant on Civil and Political Rights (ICCPR);[111] and the International Covenant on Economic, Social and Cultural Rights (ICESCR).[112] These are known collectively as the International Bill of Human Rights. The first two have relevance for any discussion on privacy and are described below.

In 1948, the publication of the UDHR set out what aimed to be a 'common standard of achievement'[113] whereby everyone in the world can work towards the goal of universal acceptance. States must both protect individuals from abuses of their human rights, while at the same time refrain from interfering with those rights themselves. Individuals must respect the rights of others.[114] Art. 12 provides a right to privacy:

> No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and

---

[110] Universal Declaration of Human Rights (adopted 10 December 1948 UNGA Res 217 A(III)) (UDHR)

[111] International Covenant on Civil and Political Rights (adopted 16 December 1966, entered into force 23 March 1976) 999 UNTS 171 (ICCPR)

[112] International Covenant on Economic, Social and Cultural Rights (adopted 16 December 1966, entered into force 3 January 1976) 999 UNTS 3 (ICESCR).

[113] UDHR (n 110) preamble

[114] See UN website <http://www.ohchr.org/en/issues/Pages/WhatareHumanRights.aspx> accessed 21 June 2010

> reputation. Everyone has the right to the protection of the law against such interference or attacks.[115]

This establishes a generic right to privacy at an international level. However, privacy cannot be absolute and Art.29 states that limits to privacy should be determined by law to ensure the protection of the rights of others, and those required to ensure 'morality, public order and the general welfare in a democratic society.'[116]

Although non-binding the UDHR paved the way for two covenants - the ICESCR and the ICCPR. The covenants gave States both a legal and a moral obligation to both promote and protect human rights.[117] It is the ICCPR, which entered into force on 23 March 1976, that provides a legal right to privacy. Although there is no requirement to directly incorporate the Covenant into domestic legislation,[118] States are to adopt laws as necessary to ensure the protections in the Covenant are recognised in their legal systems.[119]

Art. 17 of the ICCPR expands on the right to privacy as defined in the UDHR:

> No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.
>
> Everyone has the right to the protection of the law against such interference or attacks.[120]

---

[115] UDHR (n 110) Art 12

[116] UDHR (n 110) Art.29(2)

[117] UN Fact Sheet No.2 (Rev. 1) the International Bill of Human Rights, available from <http://www.ohchr.org/Documents/Publications/FactSheet2Rev.1.en.pdf > accessed 23 June 2010, 8

[118] Manfred Nowak, *UN covenant on civil and political rights: CCPR commentary* (Kehl, Germany, 2005, 2nd edn) 54

[119] ICCPR (n 111) Art.2(2)

[120] ICCPR (n 111) Art 17

The definition adds the word ‘unlawful’, meaning that interference must be neither arbitrary nor unlawful. Thus, privacy is not an absolute right. Whereas everyone may have the right to the protection of their privacy by law, equally governments are free to legislate privacy-invasive laws. The law can protect privacy, and the law can take privacy away. Where lawfully carried out, surveillance can be a legitimate invader of privacy. Nevertheless, it does serve to strengthen the right in that interference with privacy must be both purposeful *and* lawful.

The ICCPR represents a clear statement of human rights and includes the right to privacy. However, it has not gained universal acceptance, enjoying only a ‘tenuous foothold’[121] in US law and not yet incorporated into federal law. China claims to be ‘paving the way’[122] towards ratification but the process is very slow. The ICCPR will be revisited in Chapter 7.

2.2.2 The European Convention on Human Rights

As well as the International Bill of Human Rights, as a member of the Council of Europe (CoE) and signatory to the ECHR, this regional instrument takes effect in the UK. The ECHR came into effect on 3 September 1953. It consists of 59 articles, of which 13 define rights and freedoms. All member states of the CoE have signed and ratified the ECHR.[123]

Similar to the division between the ICCPR and the ICESCR, the ECHR protects mainly civil and political rights, leaving economic and social rights to

---

[121] David Kaye, ‘State Execution of the International Covenant on Civil and Political Rights’, 3 UC Irvine L. Rev. 95, 96

[122] See the statement by the counsellor of the Chinese delegation to the UN, 3rd Committee of the 65th session of the General Assembly on the Implementation of Human Rights Instruments (Item68A) (19/10/2010) <http://www.china-un.org/eng/chinaandun/socialhr/rqwt/t762572.htm> accessed 10 November 2010

[123] The current status of signatures and ratifications of the ECHR can be found at <http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=005&CL=ENG> accessed 3 September 2010

the European Social Charter.[124] States are required to ‘secure to everyone within their jurisdiction the rights and freedoms’[125] defined within the ECHR. The ECHR allows applications from individuals, but only after all domestic remedies have been exhausted.[126]

Art.19 of the ECHR established the European Court of Human Rights (ECtHR) to ‘ensure the observance’[127] of the Convention by states. States must undertake to ‘abide by’[128] the final judgement of the ECtHR.

Privacy is protected by Art. 8 of the ECHR which states:

> Everyone has the right to respect for his private and family life, his home and his correspondence.[129]

The wording of Art. 8 differs from the terms used in the international instruments. The ECHR uses the term ‘private and family life’[130] as opposed to the word ‘privacy’[131] used in the UDHR, and later ICCPR. The term 'private life' is broad and the ECHR has not considered it possible or even necessary to exhaustively define it.[132] It did, however, find it too restrictive to limit 'private life' to one's '"inner circle"'[133] - to some degree, it must also include:

---

[124] Laurids Mikaelsen, *European protection of human rights*, (Sijthoff & Noordhoff, The Netherlands, 1980) at 4.2.1 p12

[125] ECHR (n 20) Art 1

[126] Ibid., Art 34

[127] Ibid., Art 19

[128] Ibid., Art 46 (1)

[129] Ibid., Art 8(1)

[130] Ibid., Art 8 (1)

[131] ICCPR (n 111) Art 17

[132] *Niemietz v Germany* App. No. 13710/88 (ECtHR, 16 December 1992) at 29

[133] Ibid.

> the right to establish and to develop relationships with other human beings, especially in the emotional field for the development and fulfilment of one's own personality[134]

This suggests that where one has the liberty to develop intimate relationships in private one has the autonomy to develop oneself as a person. However, the right is not absolute. A wide set of criteria was specified whereby a public authority can interfere with this right:

> 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[135]

So, privacy is protected regionally, but such protection is limited in way which can be difficult to define. While the essence of the limitations may make sense, for example, to enable crime fighting, the areas are very broad. National security is perhaps the hardest to define in terms of limitation of privacy. In *Esbester v United Kingdom*[136], the court found the definition to be 'not amenable to exhaustive definition'.[137] Economic well-being is also hard to scope, given it can include diverse matters such as oil supply or espionage.[138]

However, despite the limitations set out in Art.8(2), the ECtHR applies tests to determine the legality, necessity and proportionality of any interference. The test of legality includes the need for the interference to be founded in the laws of the state concerned and that those laws must be clear and accessible to the people so they can know when their rights have been infringed.[139] The test

---

[134] *X v Iceland* App. No. 6825/74 (ECtHR, 18 May 1976)

[135] ECHR (n 20) Art 8(2)

[136] *Esbester v United Kingdom* App. No. 18601/91 (Commission Decision, 2 April 1993)

[137] Ibid.

[138] Michael Cousens, *Surveillance Law* (Reed Elsevier, 2004), 87

[139] Feldman *Civil liberties and human rights in England and Wales* (n 41) 56

of necessity checks that any interference was a ‘response to a pressing social need’[140] to take action for the given purpose, for example, national security. States have some degree of discretion when making judgements about the social need and their response – this ‘'margin of appreciation'‘[141] is allowed because state governments are better placed than the ECHR at evaluating local conditions. Proportionality balances the ‘nature and extent of the interference against the reasons for interfering’[142], taking into account, for example, whether a less intrusive method could have had the same effect.

In its resolution of 1970, the Parliamentary Assembly of the CoE stated that there can be a conflict between the freedoms of information and expression and the right to privacy, and that the exercise of those rights ‘must not be allowed to destroy the existence of’[143] privacy. It further defined the right to privacy as being the ‘right to live one's own life with a minimum of interference’,[144] and also set out the protections of the right as concerning:

> private, family and home life, physical and moral integrity, honour and reputation, avoidance of being placed in a false light, non-revelation of irrelevant and embarrassing facts, unauthorised publication of private photographs, protection against misuse of private communications, protection from disclosure of information given or received by the individual confidentially.[145]

In specifically stating that privacy concerns each of these elements, it indicates that privacy is an enabler for them. In addition, it warned of the dangers ‘computer-data banks’[146] and that a person must not become

---

[140] Ibid., 57

[141] Ibid.

[142] Ibid.

[143] Council of Europe Parliamentary Assembly Resolution 428 (1970), C.1

[144] Ibid., C.2

[145] Ibid.

[146] Ibid., C.5

'completely exposed and transparent'[147] due to the accumulation of data. It also stated that ECHR Art.8 should provide protection from interference not only by public bodies but also other people or private institutions, including the media.

In the next sections, a review of the source of privacy in the three chosen jurisdictions is made, starting with the US.

2.2.3 Sources of privacy in the US

It may be considered surprising that there is not a single reference to a general right of privacy anywhere in the US Constitution, especially as freedoms such as speech, assembly and the press are protected.[148] However, it is consistent with the view that society is a 'collection of citizens, and not a conglomerate of private individuals'.[149] Yet, the US courts have extrapolated some level of privacy protection from the various Amendments in the Bill of Rights, in particular the Fourth Amendment:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.[150]

Protection of privacy in the US has come from a variety of sources. Warren and Brandeis discussed the protection of people 'in person and in property',[151] and the way the common law had incorporated protections to 'meet the new

---

[147] Ibid., C.7

[148] US Constitution 1st Amendment

[149] Grant Mindle, 'Liberalism, Privacy and Autonomy', 51 J. Politics 1989 575 at 578

[150] US Fourth Amendment <http://www.senate.gov/civics/constitution_item/constitution.htm> accessed 6 November 2016

[151] Warren and Brandies (n 65)

demands of society'[152] as changes in society and the economy and technology progressed. Taking Cooley's immunity from assault and battery and noting that '[t]houghts, emotions, and sensations'[153] demanded equal protection in law, they considered that the right to be let alone should protect against 'the evil of the invasion of privacy'[154] by the Press, where '[i]nstantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life'.[155] Their work, described as the 'outstanding example of the influence of legal periodicals upon the American law',[156] became one of the cornerstones of US privacy protection.

The case of *Roberson v Rochester Folding Box Co.*[157] dealt with the use of a photograph of a girl in advertising. The judges ruled 4 to 3 that the right of privacy had 'not as yet found an abiding place in [US] jurisprudence'.[158] The principal objection to accepting the right was that to apply it fully would result in a 'vast amount of litigation',[159] suggesting that even the spoken word would invade a person's 'right to be absolutely let alone.'[160] However, the resultant public outcry[161] resulted in the State of New York enacting a statute to make

---

[152] Ibid.

[153] Ibid., at 195

[154] Ibid.

[155] Ibid.

[156] Prosser (n 97) 383

[157] *Roberson v Rochester Folding Box Co* 171 N.Y. 538 (1902)

[158] Ibid., 556

[159] Ibid., 545

[160] Ibid.

[161] W Page Keeton (ed), *Prosser and Keeton on Torts* (5th edn) (West, Minnesotta, 1984) p850; see for example letter to the editor New York Times 13 July 1902, <http://query.nytimes.com/gst/abstract.html?res=F10910F83A5F12738DDDAA0994DF405B828CF1D3> accessed 4 January 2011

it illegal to use the ‘name, portrait or picture of any living person’[162] in advertising or by way of trade without permission.

A later case *Pavesich v New England Life Insurance Co.*[163] dealt with a similar issue of the publication of a person's likeness. Here, the court rejected the findings in *Roberson*, accepting the view of Warren and Brandeis. The court found that the right of privacy is ‘embraced within the absolute rights of personal security and personal liberty’[164] and has its basis in natural law.[165] It continued that freedom of speech and of the press can limit privacy but must not be allowed to destroy, or to be destroyed by privacy.

In *NAACP v Alabama*,[166] the Supreme Court arrived at a ‘landmark associational privacy decision’.[167] The courts in Alabama had demanded the membership list from the National Association for the Advancement of Colored People (NAACP) who refused. It claimed it was ‘constitutionally entitled to resist official enquiries into its membership lists’.[168] The court recognised the ‘vital relationship between freedom to associate and privacy in one's associations’.[169] The court found that the rights of NAACP members ‘to pursue their lawful private interests privately and to associate freely with others in so doing’[170] came under the protection of the Fourteenth Amendment.

---

[162] New York State Consolidated Laws, Civil Rights, Sec 50 Right of privacy

[163] 122 Ga. 190

[164] Ibid., syllabus

[165] Ibid., 194

[166] 357 US 449 (1958)

[167] John Shattuck, *Rights of privacy* (National Textbook Company, Illinois, 1977) 50

[168] 357 US 449 (1958) 458

[169] Ibid., 462

[170] Ibid., 466

In the landmark case of *Griswold v Connecticut*,[171] the court determined that 'specific guarantees in the Bill of Rights have penumbras, formed by emanations from those guarantees that help give them life and substance'.[172] These guarantees create 'zones of privacy'.[173] The court found that the case involved 'a relationship lying within the zone of privacy created by several fundamental constitutional guarantees.'[174] The Fourth Amendment explicitly provides the right of people 'to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures'.[175] The Fifth Amendment's self-incrimination clause 'enables the citizen to create a zone of privacy which government may not force him to surrender to his detriment.'[176] The Ninth Amendment prevents constitutional rights from being 'construed to deny or disparage [other rights] retained by the people'.[177]

This constitutionally protected zone of privacy in *Griswold* has been enlarged to cover 'to a considerable extent'[178] personal autonomy. In *Whalen v Roe*,[179] the court recognised that privacy interests cover not only the avoidance of 'disclosure of personal matters',[180] but also enable people to independently make important decisions.[181] The former is a form of informational privacy[182]

---

[171] 381 US 479 (1965)

[172] Ibid., 484

[173] Ibid.

[174] 381 US 479 (1965) 485

[175] 4th Amendment to the US Constitution

[176] 381 US 479 (1965) 484

[177] US 9th Amendment

[178] Keeton (n 161) 866

[179] *Whalen v Roe* 429 US 589 (1977)

[180] Ibid., 599

[181] Ibid., 599 - 600

[182] Russell Gorkin, 'The constitutional right to information privacy: NASA v. Nelson', 6 Duke J. of Constitutional Law & Public Policy Sidebar, 1

while the latter is a provider of personal autonomy, which as Westin states is 'vital to the development of individuality and consciousness of individual choice in life'.[183] The *Whalen* judgement also presented a warning that although the court was not deciding on such matters, it was aware of the 'threat to privacy implicit in the accumulation of vast amounts of personal information in computerized data banks or other massive government files'.[184]

The situation in the US specifically regarding privacy and communications surveillance is given in detail in Chapter 3. The next section gives an overview of privacy within the context of the UK.

2.2.4 Sources of privacy in the UK

Unlike the US, the UK does not have a written constitution. Any protection of privacy that the law provides is 'scattered throughout civil and criminal law, both common and statute.'[185] An early example is the offence of eavesdropping - 'standing outside the walls of a house to listen to what was being said within'.[186] This defined in the Justices of the Peace Act 1361 and cases have been recorded at least as far back as the fifteenth century.[187] It has been described as conduct 'regarded as socially harmful or disruptive'.[188]

---

[183] Westin (n 42) 34

[184] Ibid., 605

[185] Home Office, *Report of the Committee on Privacy* (Cmnd. 5012, 1972) p25 s.83

[186] Marjorie K McIntosh, *Controlling misbehaviour in England, 1370 – 1600* (Cambridge University Press, Cambridge, 1998), p.9

[187] Bertha H Putnam, *Proceedings before the justices of the peace in the fourteenth and fifteenth centuries, Edward III to Richard III*, (Spottiswoode, London, 1938) p.96-97. In 1413, Thomas Smyth was accused of being an eavesdropper at numerous houses across the town of Petlyng. The Latin *asculator et obidator* translates to listener and eavesdropper.

[188] McIntosh (n 186) 9

Trespass laws can protect privacy. In *Entick v Carrington*[189], the court found that every invasion of one's private property was trespass and removal of papers aggravated this. In 1931, Winfield questioned whether there should be a tort of infringement of privacy. In *Tolley v J.S. Fry & Sons Ltd*,[190] the court 'exercised their imaginations'[191] and devised a remedy under defamation law where an amateur golfer had been falsely portrayed endorsing a chocolate product, thus endangering his amateur status. Winfield defined privacy as the:

> infringement of privacy is unauthorized interference with a person's seclusion of himself or of his property from the public[192]

This differs from defamation as there is not necessarily damage to a person's reputation, nor is there necessarily any written statement.

The tort of breach of confidence protects unauthorised disclosure of information where there was a duty of confidence. In the leading case of *Prince Albert v Strange*,[193] the case was decided in terms of breach of confidence as well as property rights.[194] However, not all personal information is confidential. For example, a person's political beliefs may be private to them but are 'not normally considered confidential.'[195]

There had been increasing concerns in the UK of the adequacy of the law to protect privacy. In 1976, Justice set up a committee to investigate privacy

---

189 *Entick v Carrington*, 19 Howell's State Trials 1029 (1765)

190 *Tolley v J.S. Fry & Sons Ltd* [1930] 1 KB 467

191 David J Seipp, 'English judicial recognition of a right to privacy', 3 Oxford J Legal Studies 3 325 at 327

192 Percy H Winfield, 'Privacy' (1931) 47 LQR 23

193 *Prince Albert v Strange* [1849] EWHC Ch J20 (8 February 1849)

194 Michael Tugendhat and Anna Coppola, 'Principles and Sources' in Michael Tugendhat and Iain Christie, (eds) *The law of privacy and the media* (OUP, Oxford, 2002), 2.12

195 Michael Tugendhat, Matthew Nicklin and Godwin Busuttil, 'Publication of Personal Information' in Michael Tugendhat and Iain Christie, (eds) *The law of privacy and the media* (OUP, Oxford, 2002), 4.15

which developed a common law tort to cover privacy.[196] It prepared a draft bill[197] which led to the establishment of the Committee on Privacy, the Younger Committee. The Committee reviewed privacy issues and determined that from the evidence it received, the main concern of privacy invasion involves the 'treatment of personal information'[198] as opposed to confidential information. Among the committee's recommendations were that there should be a tort to cover the unlawful use of surveillance devices,[199] legislation to cover the computer processing of personal information,[200] clarification of the law relating to breach of confidence,[201] and a tort of 'disclosure or other use of information unlawfully acquired'.[202] Subsequently, the government set up a committee to further discuss privacy issues. In its report of 1990,[203] the Calcutt Committee determined simply that there was no need for a tort of infringement of privacy to be introduced.[204] It did, however, make recommendations that it be illegal to enter onto or place a surveillance device on private property without consent and with the intent property, to obtain personal information, or to photograph or record anyone on private with the aim to publish the information.[205]

---

196 G Taylor, 'Privacy and the public' 34 MLR 3 (May 1971) 288-304 at 288

197 Mark Littman and Peter Carter-Ruck 'Privacy and the Law, a report by Justice', 1970, 59

198 Home Office, *Report of the Committee on Privacy* (Cmnd. 5012, 1972), 64

199 Ibid., 53(iv)

200 Ibid., 54

201 Ibid., 55

202 Ibid., 56

203 Home Office, *Report of the Committee on Privacy and Related Matters* (Cm 1102, 1990)

204 Ibid., 12.5 p46

205 Ibid., ix

Although the UK was among the first countries to sign the ECHR, it was among the last to give effect to the provisions in domestic law.[206] The Human Rights Act (HRA) took effect on 2 October 2000 and gave 'further effect to rights and freedoms guaranteed under the [ECHR]'.[207] In particular, the Act made it 'unlawful for a public authority to act in a way which is incompatible with a Convention right'.[208] However, this does not apply if the authority 'could not have acted differently'[209] due to primary legislation; or, if that legislation could not be 'read or given effect in a way which is compatible with the Convention rights'.[210]

Privacy gained further protection from the Charter of Fundamental Rights of the European Union[211] in December 2000. Art. 7 of the Charter gives the 'right to respect for his or her private and family life, home and communications.'[212] Limits to the right are provided in Art. 52 which stresses that limitations must be lawful, proportional and necessary.[213]

A clear early example of the effect of the HRA is found in *Douglas and Others v Hello! Ltd.*[214] Sedley LJ stated that the UK had 'reached a point at which it can be said with confidence that the law recognises and will appropriately

---

[206] Samantha Besson, 'The reception process in Ireland and the United Kingdom' in Helen Keller and Alec Stone Sweet (eds) *A Europe of rights: the impact of the ECHR on national legal systems*, (OUP, Oxford, 2008), 31

[207] Human Rights Act 1998

[208] Ibid., 6 (1)

[209] Ibid., 6 (2)(a)

[210] Ibid., 6 (2)(b)

[211] Charter of Fundamental Rights of the European Union, 2000/C 364/01, 18 December, 2000

[212] Ibid., Art 7

[213] Ibid., Art 52

[214] *Michael Douglas, Catherine Zeta-Jones, Northern & Shell plc v Hello! Limited*, [2000] EWCA Civ 353

protect a right of personal privacy.'[215] In reaching this conclusion, he stated that the law recognises that 'everybody has a right to some private space'[216] and that the Human Rights Act 'requires the courts … to give appropriate effect to the right to respect for private and family life'[217] as set out in ECHR Art. 8. The law can protect people who 'simply find themselves subjected to an unwanted intrusion into their personal lives.'[218] Privacy can be seen as a 'legal principle drawn from the fundamental value of personal autonomy.'[219] This case shows how there was an infringement of the claimants autonomy to determine how their personal information, in this case in the form of photographs were used. It can thus be construed that a person has the autonomy to decide how his personal information is used, and that autonomy is one of the core values that privacy protects.

2.2.5 Sources of privacy in China

China's current legal system only developed from 1978, China passing from an essentially lawless state under the control of a supreme leader to a state with a great many laws and regulations. Some of these laws and regulations were inconsistent, some only short-term, but they met the urgent need for reform and development.[220]

Several human rights are guaranteed, as set out in the 2009-2010 human rights action plan[221] but there is no explicit mention of privacy, nor is privacy

---

[215] Ibid., at 110

[216] Ibid., at 111

[217] Ibid.

[218] Ibid.,126

[219] Ibid.

[220] Yuwen Li and Jan-Michiel Otto, 'Central and Local Law-Making: Studying China's Experience', in Eduard Vermeer and Ingrid d'Hooghe (eds) *China's Legal Reforms and Their Political Limits* (Curzon, Richmond, 2002), 1

[221] Information Office of the State Council of the People's Republic of China: National Human Rights Action Plan of China (2009-2010)

mentioned in the 2012-2015 National Human Rights Action Plan.[222] Some limited rights to privacy can be found in the Constitution of the PRC. It is prohibited to make an 'unlawful search of the person of [a] citizen'[223] and an '[u]nlawful search of, or intrusion into, a citizen's home'.[224] Such unlawful searches are a criminal offence.[225] However, Ong finds that privacy protection in China is 'not comparable'[226] to that in the West; it lacks a 'comprehensive and coherent system'[227] for the protection of privacy. Wang finds China to be 'at least 30 years'[228] behind the West with regard to privacy.

Correspondence gains more attention, with 'freedom and privacy of correspondence'[229] being protected except where necessary for the purposes of state security or criminal investigation. The available action is censorship, though to enable this the correspondence must be examined. The unlawful opening of letters is a criminal offence.[230] This postal definition of

---

[222] Information Office of the State Council of the People's Republic of China: National Human Rights Action Plan of China (2012-2015)

[223] Constitution of the People's Republic of China (updated 14 March 2004), Art 37 <http://www.npc.gov.cn/englishnpc/Constitution/2007-11/15/content_1372964.htm> accessed 28 September 2010

[224] Ibid., Art 39

[225] Criminal Law of the People's Republic of China <http://www.npc.gov.cn/englishnpc/Constitution/2007-12/13/content_1384075.htm> accessed 28 September 2010, Art 245

[226] Rebecca Ong, 'Recognition of the right to privacy on the Internet in China', 1 International Data Privacy Law 3, 2011, 172

[227] Ibid.

[228] Hao Wang, *Protecting Privacy in China: A Research on China's Privacy Standards and the Possibility of Establishing the Right of Privacy and the Information Privacy Protection Legislation in Modern China* (Springer, Berlin, 2011), preface v

[229] Constitution of the People's Republic of China (n 223) Art 40

[230] Criminal Law of the People's Republic of China (n 225) Art 252

correspondence is similar to the way the law in the US and UK developed pre-Internet and is far from a general protection of privacy.[231]

The Constitution also offers protection of personal dignity,[232] specifically from wrongs such as libel and false accusation. As was discussed above, a person's dignity is one area protected in general by that person's privacy. This has been described as the 'ultimate source'[233] of the protection of personal rights. Yet, for all the protections in the Constitution, it clearly sets the State above the person, as people 'may not infringe upon the interests of the State, of society or of the collective'[234] while exercising their rights and freedoms. In China, the rights of the government always take precedence over the rights of the individual.[235]

Civil law includes protection for people's name,[236] portrait,[237] reputation[238] and honour,[239] and has recourse in law against infringement of these.[240] These are restated as 'personal and property rights and interests'[241] in the Tort

---

[231] Hong Xue, 'Privacy and personal data protection in China: an update for the year end 2009', 26 Computer Law & Security Review 284 at 285

[232] Constitution of the People's Republic of China (n 261) Art 38

[233] Guobin Zhu, 'The Right to Privacy: An Emerging Right in Chinese Law', 18 Statute L. Rev. 3 1997, 208-214, 211

[234] Constitution of the People's Republic of China (n 261) Art 51

[235] Wang (n 228) 51

[236] General principles of the civil law of the People's Republic of China, Art 99, <http://www.npc.gov.cn/englishnpc/Law/2007-12/12/content_1383941.htm> accessed 28 September 2010

[237] Ibid., Art 100

[238] Ibid., Art 101

[239] Ibid., Art 102

[240] Ibid., Art 120

[241] Tort Liability Law of the People's Republic of China, Art.2, <http://www.npc.gov.cn/englishnpc/Law/2011-02/16/content_1620761.htm> accessed 19 January 2017

Liability Law of the PRC, which came into force on 1 July 2010. In addition, the Tort Liability Law specifically includes the 'right to privacy'.[242] The remedies provided by this Law include '[c]ompensation for loss',[243] 'formal apology'[244] and the 'elimination of ill effects and the restoration of reputation'.[245] The Law does not expand on what privacy may mean but Greenleaf states that this will most likely cover 'violations of personal information or data privacy'.[246]

2.2.6 Summary

Privacy, up until now, has been discussed primarily from a theoretical standpoint. The research findings show that it enables personal autonomy and helps to maintain a person's dignity and liberty. It enables us to be who we are. It is not only spatial but also concerns personal information. It can be lost, given away or taken. Once gone, it cannot be recovered.

As a concept, however, as shown in this research privacy is 'not universally regarded as fundamentally important.'[247] Some of the aspects of privacy described above are not compatible with some forms of government or society;[248] thus, privacy would not simply happen unaided.

Also, the research findings show that there are diverse meanings of privacy as well as different levels of protection both nationally and internationally.

---

[242] Ibid.; note that some translations give the "right of privacy", see for example <http://www.wipo.int/wipolex/en/text.jsp?file_id=182630> accessed 19 January 2017

[243] Ibid., Art 15(6)

[244] Ibid., Art 15(7)

[245] Ibid., Art 15(8)

[246] Graham Greenleaf, *Asian Data Privacy Laws: Trade and Human Rights Perspectives* (OUP, 2014), 202

[247] David Feldman, 'Privacy-related rights and their social value', in Birks, P., (ed) *Privacy and Loyalty* (Clarendon, Oxford, 1997), 2

[248] Ibid.

Although privacy can be invaded by the prying eye of one's neighbour or the thirst of the media for a story, government Internet surveillance is put forward as the greatest threat to informational privacy.

Furthermore, surveillance, or more specifically government surveillance is an article of control. It has been described as the 'antithesis of privacy'[249] and the 'polar opposite of democracy'.[250] Describing the struggle against surveillance Westin wrote:

> [t]he effort to limit official surveillance over man's thoughts, speech, private acts, confidential communications, and group participation has for centuries been a central part of the struggle for liberty in Western society. This search for personal and group privacy has been waged against kings and legislatures; churches, guilds, manor lords, and corporations; sheriffs, welfare investigators, and political police.[251]

Surveillance affects autonomy and liberty as defined above. It affects one's ability to be anonymous, and where one lives in fear of surveillance one may lessen one's interactions with others. In this way it affects our liberty. Surveillance can be used to acquire our personal information and it is this which is transmitted in so many ways and for so many purposes when we make use of the Internet.

The next section begins to examine the Internet from a functional perspective in order to aid the understanding of how and where privacy may be invaded. This provides a background to enable discussions provided and depicted in Chapter 6.

---

[249] Ann Cavoukian, International Council on Global Privacy & Security by Design, <http://gpsbydesign.org> accessed 25 January 2017

[250] Kevin D Haggerty and Minas Samatas, 'Surveillance and democracy: an unsettled relationship' in Kevin D Haggerty and Minas Samatas (eds.) *Surveillance and Democracy* (Routledge-Cavendish, Oxon, 2010) p1

[251] Westin (n 42) 67

2.3 The Internet and privacy risks

The previous sections of this chapter have discussed the definition of privacy itself, as a concept and also in the context of international law. This section now focuses on the Internet from a technical perspective in order to help understand the various ways that privacy can be invaded or indeed protected.

Personal information is often exposed when privacy is invaded or discarded. For any investigation into Internet privacy to have context, it is important to first examine how data flows within the Internet and for this it is first necessary to understand in simple terms how the Internet functions. Technical issues and possibilities are often overlooked by lawmakers drafting legislation which is written in terms which are either too broad or too specific as will be seen in the following chapters. The basic technical knowledge set out below will help to understand these issues. It will be expanded upon in Chapter 6.

2.3.1 Privacy and the Information Society

Lessig defines privacy as that part of one's life which can be neither monitored or searched. Monitoring, in a social setting is simply being watched as one goes about one's business. A person may be noticed but unless their behaviour is not normal that notice will be transient. What constitutes normal behaviour is defined by the society itself to become social norms.[252] These social norms will be revisited in Chapter 7. The part of one's life which can be searched basically includes anything which is written down or recorded in some way. Private material held in the home is protected by trespass laws and those laws which limit searches by the state.[253] However, where the Internet is concerned we see monitoring and searching come closer together. Lessig uses the term 'architecture'[254] to indicate the structures and technologies in place, be it those of a small town where monitoring is personal

---

[252] Lawrence Lessig, 'The Architecture of Privacy', 1 Vand. J. Ent. L. & Prac. 56 1999, 57-58

[253] Ibid., 58

[254] Ibid., 57

and transient to that of the Internet where it becomes a permanent record which can then be searched. The architecture of a discussion between two people in a private room is very different from that of a discussion between those same people in separate private rooms using the Internet as a communications channel. Whereas the communicating parties may consider themselves secluded by virtue of them using computers located in private spaces, the walls of the private room have gone and the architecture now permits monitoring and subsequent recording. That recording creates a 'digital footprint'[255] which can be searched.

Control over our personal information gives us informational privacy. According to DeCew this includes information about a person's 'daily activities, personal lifestyle, finances, medical history, and academic achievement'.[256] DeCew's view of informational privacy is in line with the definition of personal information proposed by Wacks (as discussed in Section 2.2, page 21). All are examples of information which that person need not divulge or expect to be divulged by others. Tavani adds that informational privacy is the control over and/or limiting of access to any personal information that is stored or communicated electronically.[257] Echoing Westin's definition of informational privacy (as discussed in Section 2.2, page 21) it includes information communicated across the Internet.

Even before the Internet became widespread there were concerns about informational privacy. In the US people were becoming concerned with data processing. Social scientists had recommended the development of a national computer centre to hold data collected by government agencies including the

---

[255] Spencer Kelly, 'The spread of our digital footprint' <http://news.bbc.co.uk/1/hi/programmes/click_online/7380645.stm> accessed 18 January 2011

[256] Judith Wagner DeCew *In Pursuit of Privacy: Law, Ethics, and the Rise of Technology* (Cornell University Press, New York, 1997) 75

[257] Herman T. Tavani 'Informational Privacy: Concepts, Theories, and Controversies' in Kenneth Einar Himma and Herman T. Tavani, (eds)*The Handbook of Information and Computer Ethics* (Wiley, New Jersey, 2008) 139

census. This resulted in public outcry and congressional scrutiny.[258] With the additional catalyst of the Watergate scandal the Privacy Act of 1974[259] was passed. However, the Act only regulated information held by the federal government and its agencies. This Act then has no great effect on the protection of informational privacy in general.

Discussion on data protection in the UK can be traced to the 1978 Lindop committee which proposed a framework within which to find a balance between the protection of and use of personal information.[260] Put simply, data needs to be used in order to be of use. The committee established a forward-looking definition of personal data as 'any data which relate, or which can be related, to an identified or identifiable individual, including the data whereby he can be identified'.[261] Were this put into a modern Internet context, it would protect not only personal information but also communications metadata as this can be used to identify an individual. As a result, the UK government passed the Data Protection Act 1984 (DPA84), 9 years after the US Privacy Act became law. However, personal information gained no protection by the Act if access were required to safeguard national security.[262]

2.3.1.1 EU Data Protection

One benefit of the Internet, in particular since the invention of the Web coupled with advances in communications technology and availability, is that it created a global space for everything from the sale of goods and services, to access to government, news and information services. Through this, the world

---

[258] Rebecca S. Kraus 'Statistical Dèjá Vu: The National Data Center Proposal of 1965 and Its Descendants' 5 J. Privacy & Confidentiality 1 (2013) 1-37

[259] Privacy Act of 1974, Pub. L. 93–579, 88 Stat. 1896, December 31, 1974

[260] Home Office, *Report of the Committee on Data Protection* (Cmnd. 7341, 1978), at summary 02, xix

[261] Ibid., 38.01

[262] Data Protection Act 1984, 27

entered the 'age of the Information Society.'[263] The free flow of data, including personal information within the Information Society is vital for its operation and this was hampered by different data protection laws within the members of the EU. This was addressed by the Data Protection Directive on 24 October 1995[264] which created a formal regime with no barriers to the free flow of personal information between member states. The right to the protection of personal information was also incorporated into Art. 8 of the Charter of Fundamental Rights of the European Union.[265] The UK incorporated the Directive via the Data Protection Act 1998 (DPA) which repealed DPA84, coming into force on 1 March 2000.[266] Again, the DPA provides no protection in cases of national security.[267]

Harmonised data protection across the EU now meant data could be transferred freely and yet, a provision had to be made to cater for the transfer of data to non-EU countries and that was done by Art. 25. This required that the country where the data was to be transferred to had adequate data protection.[268] This presented a problem where the US was concerned. The US approach to data protection regulates government intrusion whereas the EU approach covers the protection of personal data in general and business use in particular. While protections in the US may be considered adequate in

---

[263] House of Lords Select Committee on Science and Technology 5th Report, 1996, HL 77, 1.6; see also Yaman Akdeniz, Clive Walker and David Wall, *The Internet: law and society* (Pearson, Harlow, 2000), 3

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

[265] Charter of Fundamental Rights of the European Union, 2000/C 364/01, Art 8(1)

[266] The most significant difference between the 1984 and 1998 Acts is the inclusion of paper-based filing systems in the later Act. Both Acts protected computerized personal data in a similar way.

[267] Data Protection Act 1998, Art. 28

[268] Data Protection Directive (n 264) Art 25(1)

some areas, it is, in general, inadequate.[269] To cater for this the Safe Harbor Agreement was put into place in July, 2000 enabling personal information to be transferred to the US.[270] This agreement will be revisited in Chapter 7.

2.3.1.2 Evolving EU data protection law

The Directive had been debated during the period when the Internet was moving from a little known to a widely accepted and used resource. The introduction of new digital technologies for the development of the information society resulted in the Directive 97/66/EC[271] which added new requirements to the Data Protection Directive. However, with technology changing fast the EU carried out a major review of the legislation.[272] During both the discussion and implementation phases of the Directive the World Wide Web was created and expanded rapidly. Uses of personal data were to expand and continued to do so, and legislation drafted while the Web was in its infancy simply could not predict how things would change. The Directive on Privacy and Electronic Communications[273] was the outcome of the review. It repealed 97/66/EC because of the need to provide protection across all electronic

---

[269] Gregory Shaffer, 'Globalization and Social Protection: The Impact of EU and international Rules in the Ratcheting Up of U.S. Privacy Standards', 25 Yale J. Int'l L. 1 2000, p26

[270] Commission Decision 2000/520/EC of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbor privacy principles and related frequently asked questions issued by the US Department of Commerce (OJ 2000 L 215, p.7)

[271] 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, recital 3

[272] Andrew Charlesworth, 'Information Privacy Law in the European Union: E Pluribus Unum or Ex Uno Plures?', 54 Hastings L. J. 931 2002-2003, p931

[273] 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

communications services regardless of the technology.[274] Art. 5 of the Directive addresses confidentiality of communications, prohibiting unconsented surveillance,[275] except where this is a business need, for example, for billing purposes,[276] and creates the requirement that users are to be informed of and can consent to information being stored on or read from their devices unless a service could not be delivered otherwise.[277] Art. 15 permits Member States to retain communications metadata for a limited but unspecified time.[278] Art. 5(3) was modified by Directive 2009/136/EC[279] to require prior informed consent before information was written to or read from a user's device.[280] This change became known as the *cookie law*. Cookies and other forms of tracking are discussed and presented in Chapter 6.

2.3.1.3 Updating EU data protection

In January 2012, the EU published a communication[281] discussing the challenges to data protection caused by globalisation and rapid technological

---

[274] Ibid., recital 4

[275] Ibid., Art. 5(1)

[276] Ibid., Art. 5(2)

[277] Ibid., Art. 5(3)

[278] Ibid., Art. 15

[279] Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communication networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws

[280] Ibid., Art. 2(5)

[281] Communication from the Commission of the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, 'Safeguarding Privacy in a Connected World: a European Data Protection Framework for the 21st Century' COM (2012) 9 final, 25/01/12

change. This resulted in the General Data Protection Regulation (GDPR)[282] which will become law across the EU on 25 May, 2018[283] and will repeal Directive 95/46/EC.[284]

Art .17 of the GDPR implements the right for a person to have their personal data erased in certain circumstances and is known as the 'right to be forgotten'. This provides the right to have data deleted where it is no longer required for the purpose for which it was collected provided that data is not required for freedom of expression or for legal obligations. It could not, therefore be used to delete data held under data retention legislation.[285] The right to be forgotten was first defined as a result of the Court of Justice of the European Union (CJEU) decision in *Google Spain v AEPD*[286] where the Court ruled that Google must remove links to material about the complainant. Although the case was specific to search engine indexes Art. 17 is wider in that it may target personal data held anywhere. It also imposes the duty on the data controller to inform any other controllers to which the relevel personal data has been sent of the erasure requirement provided this is both possible and the effort is not disproportionate.[287]

A person may also object to their data being processed which places the burden on the data controller of proving that the legitimacy of the processing

---

[282] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (GDPR)

[283] Ibid., Art 99(2)

[284] Ibid., Art 94

[285] Ibid., Art 17

[286] C-131/12 Google Spain, S.L., Google Inv. v Agencia Española de Protección de Datos, Mario Costeja González

[287] GDPR (n 282) Art. 19

overrides the person's right to object to it.[288] Equally, a person may require the data controller to restrict processing of their personal data.[289]

A further protection in the GDPR is the requirement that data controllers implement technical and organisational measures to ensure that data protection is fully considered in the design of systems, and that by default only necessary data is processed. Art. 25[290] points to methods such as data minimisation and pseudonymisation.

As with previous legislation national security purposes still bypass all protections.[291] However, the GDPR also has significant implications not least in the maximum fines available – the higher of €20M or 4% of the controller's total worldwide annual turnover for the previous financial year. Taken together, the right to be forgotten, the requirement of data protection by design and default, and the large fines has the potential to reduce the amount of personal data being held, which itself makes for less data to be made available to law enforcement agencies.

Data protection alone does not offer a viable solution to the loss of informational privacy due to mass Internet surveillance. The exclusion of protections for national security purposes still means that the government can access personal information from company databases and other sources as required and the legislation which permits this access sometimes lacks sufficient safeguards. This will be examined in later chapters. It is first necessary to understand the architecture of the Internet at as basic level. The architecture of the Internet is such that it has to know where data comes from and where it is going to in order to operate. It is not concerned with what that data is, some of which will be our personal information. In order to be able to visualise where such information may be at risk while in transit across the

---

[288] Ibid., Art 21

[289] Ibid., Art 18

[290] Ibid., Art. 25; see also Recital 78

[291] Ibid., Recital 16

Internet or at rest on connected servers, the next section examines the Internet from a technical perspective. It is necessary to describe in some depth how the Internet functions in order to better understand privacy risks associated with its use. This knowledge gap is constantly ignored by lawmakers who draft legislation with no real reference to underlying technologies and capabilities. Knowledge of the technicalities – or architecture of the Internet as a whole will aid the understanding of issues brought into the public realm by the 2013 Snowden revelations. One must be conscious that the Snowden revelations stem from secret documents, the validity of which cannot be ascertained as a result. However, given the understanding of the underlying technologies presented in the next section and Chapter 6 one can see that the revelations are entirely plausible.

2.3.2 Internet structure

In its simplest form, the role of the Internet is to transfer data between connected devices, be those personal computers, mobile devices, web servers or any other form of device. It has been described as a collection of networks and interconnections that functions as a 'single, cooperative virtual network'.[292] At its base level, it may simply be considered a mixture of links and interconnections which combine together to form a global mesh. Although this mesh is complex, Internet users do not see, nor do they need to know this complexity.

A useful analogy is to view the Internet in a similar way to the road network. A map of all roads in the UK will indicate a number of possible routes, say, from an address in London to one in Glasgow. If each section of road represents a link and each intersection a router, one can see two things: one can find a route between these two addresses; and that route consists of a series of intersections, each one of which requires some direction. By further applying this analogy to a courier service, the method of data communication can be

---

[292] Douglas E Comer, *Interworking with TCP/IP: Volume 1; principles, protocols and architecture* (Prentice-Hall, US, 1991), 493

defined in the same way as a letter being delivered directly.[293] A courier needs three pieces of information in order to collect and deliver the letter: the collection address; the delivery address; and a route. In this analogy, these three pieces of information are the address of each house plus the roads to take and directions for each intersection.

Similar to a postal address which defines where a building is and enables one to find it, Internet devices also need addresses, and the basic address used on the Internet is the Internet Protocol (IP) address.[294] It is this address which can be thought of as the postal address in the above analogies.[295]

The data being passed across the Internet is of no common size. It may be just a few characters such as a login name, or a large file such as a movie. In order to cater for data of any size, the data is broken down into pieces known as packets before it is sent across the Internet. These data packets pass across the Internet from origin to destination via routers which determine where the data needs to be sent to reach its destination.[296] Routers are used as intersections on the Internet sending data down the correct path in order to continue on its journey. Each data packet contains the IP address of both the sender and receiver, and this enables all routers along the path to determine where next to send the data, and also where the data came from. Using the

---

[293] We imagine a courier service here which takes a letter from A and delivers it to B with no stops. The postal service is a poor analogy in this case as there are stops, or sorting offices along the way. The postal service is, however, a perfect analogy for e-mail and is used below.

[294] There are currently two versions of IP address in use, version 4 (IPv4) and version 6 (IPv6). IPv4 addresses are 32 bits long resulting in around 4.3 billion possible addresses. These are running out. IPv6 addresses are 128 bits long, resulting in 340 trillion trillion trillion individual addresses.

[295] IP addresses for home users are typically not fixed, but the IP addresses concerned must actually relate to the sender and receiver while the transmission takes place.

[296] Although technically two communicating systems can be directly connected together, without at least a router between the two systems they cannot be connected to the Internet.

road analogy above, a router can be seen as a road intersection manned by someone directing traffic who asks each car where it is headed and directs it down the relevant road, and so on. If a road becomes closed, that person can direct the car along a different road to bypass the road closure; the Internet is resilient in that if a link becomes unavailable it can send the data via a different route. However, the road analogy is not entirely correct in one respect. Data flowing across the Internet may not take the most direct route. This may be because of arrangements between Internet Service Providers (ISPs) and their own upstream providers. It may be that a provider has spare capacity on one route and not another, or that to send data along one route simply costs less. The analogy can be brought back into line by considering, for example, a situation where a car satellite navigation system suggests an alternate route because of traffic conditions or road tolls. Internet routing will be examined further in Chapter 6.

As was outlined above, data is broken into packets before it is sent across the Internet. Referring to the courier analogy, ten couriers may be needed to take all the letters from the London house to the house in Glasgow. These letters are sequential in that they must arrive at their destination in the order in which they were sent. The ten couriers may follow in convoy, but this may not be the case. At the extreme, each of the ten couriers may be directed along a different set of roads but provided each letter is numbered they can be assembled in the correct order when they arrive at the destination. This analogy highlights two important facts about the Internet: the Internet is responsible for routing information between devices connected at its edge, and users need not understand the mechanism involved; and someone positioned at an intersection intercepting each courier that passes their way may not reveal the complete message split across the ten letters if not all of them pass the same way. However, if one has access to the ISP via which the user connects, then all data sent by or received by that user is accessible. In the courier analogy, this would be the same as stopping each courier just after the collect each letter but before they reach the first road junction. On the other hand, if one controls all the people directing traffic all the intersections, they could then examine each letter as it passes along. Although this is far more complex it is nonetheless achievable given sufficient resource. It becomes

easier if you have the resources of the intelligence agencies, as was indicated in the Snowden revelations of 2013.

One final analogy is required in order to complete our road-based understanding of the Internet. The above analogy works well when viewing a country-wide Internet, but the Internet mesh alters in structure as it passes across national boundaries, and in particular where those boundaries are complicated by the intervening geography. An example is data passing between the US and the UK which will flow across one of a comparatively small number of submarine fibre optic cables connecting the two countries. A useful analogy here is a container ship travelling across the Atlantic.[297] If our couriers are now carrying letters between addresses in London and New York, the use of the roads in each country is the same as before until they reach the sea. Here, all the couriers must board a ship for the passage across the Atlantic. This is, therefore, an ideal place in which the examine all of the letters and thus access the full content spread between them. Referring again to the Snowden revelations, the ability of intelligence agencies to tap into these cables will be examined in detail in Chapter 6.

These boundaries are also the ideal place to apply filtering and blocking technologies and we see this in effect in China. It is clear that the Internet, in particular since the advent of the web, gives access to vast amounts of information on every subject imaginable and the potential to communicate with individuals or groups anywhere. Yet, the free flow of information is 'politically contradictory'[298] to communist regimes such as China. The control over what information is available to its citizens is of particular importance of these nation

---

[297] This analogy is more useful here than air mail as in the latter case there are thousands of aircraft carrying air mail, but comparatively few ocean freighters. In addition, there are hundreds of airports but only a few sea ports. For this reason, the sea freight analogy better matches the submarine cable structure.

[298] Richard Cullen and Pinky D W Choy, 'The Internet in China', 13 Colum. J. Asian L. 99 1999, p109

states where a political party desires to maintain its monopoly.[299] From the time China first became connected to the global Internet, it sought to control external connectivity.[300] The Internet structure that China formed offers it a great deal of latitude for control. The tiered structure, with a small number of international gateways connected via Internet Access Providers (IAPs) to ISPs and then on to customers imposes points at which control and surveillance can easily be implemented. The effect of having all international Internet traffic pass through a limited number of gateways in China is that she was then in a position to implement a country-wide firewall which is discussed later in Chapter 5.

From the above one can see that one's data, including personal information is transmitted from, say a PC or smartphone to a website across defined links and intersections, any one of which can potentially be used as a tapping point to access that data for surveillance purposes. The next section looks deeper still into the technology and workings of the Internet. This is essential and important as it enhances deeper understanding of privacy risks associated with the operation of the Internet which cannot be easily evaluated with superficial knowledge.

---

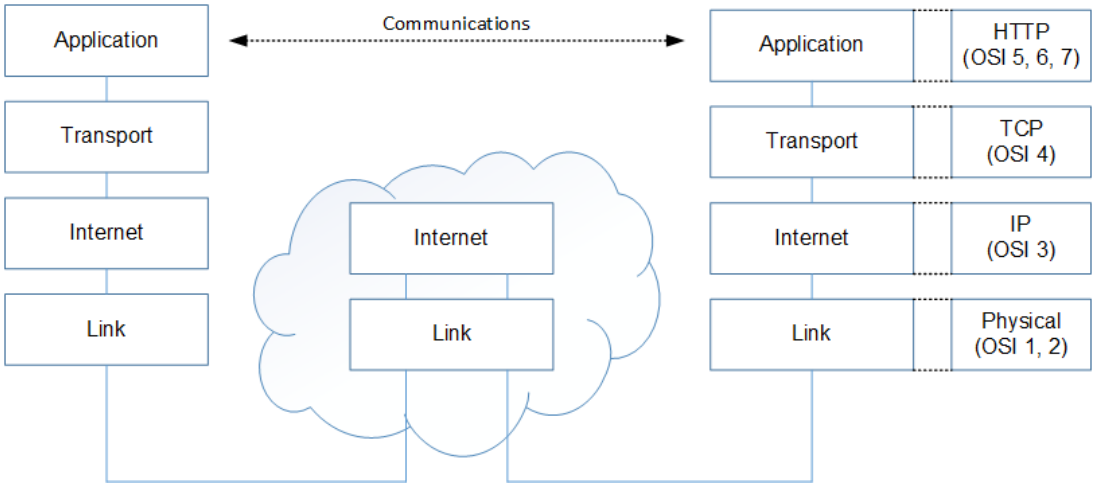
[299] Tamara Renee Shie, The Tangled Web: does the Internet offer promise or peril for the Chinese Communist Party?, J Contemporary China (2004) p524; the 1989 Student Democratic Movement protests in Tian'anmen Square saw dissidents communicating via fax machine, a 'new' technology at the time that was not State regulated. See Richard Cullen and Pinky D W Choy, 'The Internet in China', 13 Colum. J. Asian L. 99 1999, 109-110 and Trina K Kissel, 'License to Blog: Internet Regulation in the People's Republic of China', 17 Ind. Int'l & Comp. L. Rev. 229 2007, p231-232

[300] Greg Walton, *China's golden shield: corporations and the development of surveillance technology in the People's Republic of China*, (International centre for human rights and democratic development, Canada, 2001) p9

2.3.3 Data network communication

In order to send data across the Internet, a structure must be imposed. This structure is defined by the Internet Protocol (IP).[301] The protocol can be viewed as having several layers, with data passing through these layers. The function of each layer is indicated in the following diagram.

Figure 2.1: Internet Protocol layers



IP addresses were discussed above. As can be seen in Figure 2.1, these are used at the Internet layer.[302] Figure 2.1 also shows a device which only implements the Internet and Link layers. This is a router. The fact that a router only implements the lower two layers of the protocol is key to understanding Internet privacy issues. Because content exists at the top layer, a router has no access to content at all. All it has access to and indeed all it needs access

---

[301] Robert Braden, 'Requirements for Internet Hosts – Communication Layers', RFC1122, <http://tools.ietf.org/html/rfc1122> accessed 18 January 2017

[302] Note there is another model – the Open Systems Integration (OSI) model which defines the protocol in seven layers and these are included for reference. It is common for manufacturers to discuss products in terms of the 7-layer model but in an Internet Protocol context; thus, a web server at the applications layer in IP terms is OSI layer 7.

to is the IP address information. Any network device which needs access to content must therefore implement the full protocol stack.[303]

While an IP address is used to route information across the Internet, there is another form of address used by TCP and UDP which exists at the Transport layer. This address is referred to as a port. Ports are vital because they permit several applications to run on a server or a user's device at the same time. In this way, the IP address defines which server to connect to, and the port defines which service on that server is required. Without these ports one could only run one Internet application at a time; ports on a client enable any number of web browsing sessions, email clients and other applications to run concurrently.[304] However, these ports play another important role within the Internet itself and this is described next.

2.3.4 Network Address Translation

Every communicating system on the Internet requires a unique public IP address. However, the current addressing scheme, IPv4 is limited and it is impractical to allocate a public IP address to every device in the home. IPv4 addresses take the form of 4 numbers separated by dots; for example, 129.11.155.71. To cater for this the global IP address space has a series of ranges which are classed as private.[305] Public IP addresses can be routed

---

[303] It should be noted, however, that some network devices do use the upper layers. In particular, content switches and web caches which are used to speed up or to minimise data flows will use all the layers as they need access to the content itself.

[304] Defined port numbers are maintained by IANA and can be found at < http://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xml> accessed 17 February 2013; web servers typically use port 80 for plain text (http) and port 443 for encrypted (https) communications.

[305] There are several ranges of IPv4 addresses reserved for private use. These cannot be routed across the Internet. For example, the private IP address 192.168.1.1 may be used in thousands of home broadband installations. There can never be a clash as the address can never be used in the public Internet itself. See Yakov Rekhter, Robert Moskowitz, Daniel Karrenberg and Geert de Groot, Address Allocation for Private Internets, RFC1918, <https://tools.ietf.org/html/rfc1918> accessed 18

across the Internet; private ones cannot. The effect of this is that the same private IP address range can be used in every home – there will never be a clash because they can never be routed publically. Ports enable this to happen. A home broadband router will be allocated a public IP address by the ISP. Devices in the home are allocated a private IP address, typically dynamically, meaning that any given device may not always have the same private IP address.[306] When a device in the home starts to communicate with an Internet service the router uses Network Address Translation (NAT)[307] to allocate a distinct port to that communication. In this way, a number of devices in the home, each running a number of applications can all communicate with Internet services over the single public IP address. The public Internet can be thought of as ending at the home router, with a wholly private Internet being used within the home.

NAT is an important aspect of the modern Internet when considering the privacy, or otherwise of IP addresses because clearly the IP address seen from the outside cannot be used to identify a particular device in the home. This is considered further next.

2.3.5 Privacy implications of an IP address

Taken alone, an IP address by itself has little privacy implication. When combined with other publically available information it can reveal locational

---

January 2017. RCF1918 defines three network address ranges (10.0.0.0 to 10.255.255.255, 172.16.0.0 to 172.31.255.255 and 192.168.0.0 to 192.168.255.255)

[306] IP addresses are typically allocated via a protocol called Dynamic Host Configuration protocol (DHCP) and in a typical home setup DHCP will be running within the broadband router.

[307] NAT as defined by RFC3022 consists of Basic NAT which translates IP addresses, and Network Address and Port Translation (NAPT) which deals with port mapping. Together these are termed Traditional NAT. NAT alone is used here because it is commonly referred to as such. See generally Pyda Srisuresh and Kjeld Egevang, RFC3022 https://tools.ietf.org/html/rfc3022 accessed 2 December 2016

information and sometimes even a postal address.[308] When combined with non-public information an IP address can reveal customer information; the customer's ISP will record allocated IP addresses against billing and time information. However, identifying an actual person from an IP address is problematic.

In the NAT example outlined above the NAT information, that which would indicate which device in the home was communicating with what system on the Internet is often not available for inspection and even if it were there may be no logs to show which device had an IP at any given time.[309] Externally, regardless of what device within the home is communicating across the Internet the only visible IP address will be that of the home broadband router's public interface.[310] Given the public IP address of the router the relevant ISP will be able to determine the street address, but no more than that.

Just as knowledge of only a street address cannot reliably be used to identify a specific person within a property, nor can the public IP address in a home broadband setup identify the person actually using the devices connected within. Even if one could identify the device one may still not be able to identify who was using that device. This has been tested in the courts. In *Media CAT v Adams and ors.*, it was found that although Media CAT were monitoring IP addresses accessing material, the IP address only identified the person who had a contract with an ISP, not the actual person accessing any material[311]

---

[308] Public sources of information include 'whois' which can reveal the postal address of the owner of an IP number (the home broadband user is not the owner, the ISP is); 'traceroute' which can reveal the network path between devices and can thus be used to determine the ISPs involved; and geolocation websites which attempt to locate an IP address geographically.

[309] Some home broadband routers do give this information but rarely keep historic logs

[310] Joshua McIntyre, 'Balancing expectations of online privacy: why Internet Protocol (IP) addresses should be protected as personally identifiable information', 60 DePaul L. Rev. 895 2010-2011, p901

[311] [2011] EWPCC 6, at 28

who may not have even been at the same premises if the wireless network (Wi-Fi) was insecure.[312] This last point is widely acknowledged; for example, the issue of use of someone else's Wi-Fi to infringe intellectual property rights was raised by TalkTalk in response to an inquiry in 2009;[313] T-Mobile stated that finding an individual using a public IP address via a mobile network cannot be done with any degree of certainty.[314] In the US, in *K-Beech, Inc. v John Does 1-37* it was found that 'it is no more likely that the subscriber to an IP address carried out a particular function … than to say an individual who pays the telephone bill made a specific telephone call.'[315] In Europe, in *Delfi AS v Estonia*, the court determined that even if it were 'able to identify the IP address of a computer and the address where the computer was located, it was extremely difficult to identify the person'[316] using that computer.

The issue of an IP address being combined with other information to identify a person was also tested in the CJEU. Here, it was found that a dynamic IP address could be regarded as personal information where a provider legally had the means to identify a person using additional information provided by the relevant ISP.[317]

These cases still leave uncertainty. On one hand, courts are denying the use solely of an IP address to identify a person. On the other hand, the fact that a dynamic IP address may be considered personal information suggests that in some cases the courts will accept that an IP address does identify a person

---

[312] [2011] EWPCC 6 Media CAT Limited v Adams & Others at 30

[313] All Party Parliamentary Communications Group ' "Can we keep our hands off the net?" Report of an Inquiry by the All Party Parliamentary Communications Group', October 2009, 34

[314] Ibid., 35

[315] *K-Beech, Inc. v John Does 1-17*, CV 11-3995 (DRH) (GRB) Document 39, at p6

[316] *Delfi AS v Estonia* App no 64569/09 (ECtHR, 10 October 2013)

[317] Case C-582/14 *Patrick Breyer v Bundesrepublik Deutshland* (Second Chamber, 19 October 2016), 49

but does not specify how this may be achieved. Adding to this dilemma there are two versions of IP address in use on the Internet today: IPv4 and IPv6, the latter using a more complex addressing scheme of 128-bits, for instance, 2a02:c7d:3c4a:a00:d565:e02:8ef4:c21b. IPv6 has the potential for every device to have its own, globally unique IP address. IPv6 is considered an enabler of the Internet of Things (IoT).[318] This uniqueness causes an issue for Internet privacy in that it can be used to show a specific device made a specific communication. IPv6 addresses are generated using the Media Access Control (MAC) [319] address of the device which is unique to a given device. This could be used to identify an actual device as its owner travels across the globe, a fact not possible with IPv4. However, the drafters of the IPv6 specification took this into account. IPv6 has a privacy extension which enables the creation of addresses which still have a global scope but which change over time and are not related to the hardware address.[320]

While IPv6 has the potential to identify every device connected to the Internet it is some way from becoming ubiquitous. From a mass Internet surveillance perspective provided the privacy extension is enabled the actual communicating device cannot be confirmed without physical access to that

---

[318] The Internet of Things refers to the increasing number of devices connecting to the Internet to serve people. For example, refrigerators which can monitor their contents and place orders for supplies without human intervention. As such devices become commonplace the rate at which the IPv4 address space is running out will accelerate.

[319] Specifically, the MAC address is split and the hexadecimal FE inserted in the middle. The local/global bit is set to 1. This is then used to form a part of the IPv6 address. Take for example the MAC address 11:22:33:44:55:66, inserting FE creates 11:22:33:FE:44:55:66 and setting the local/global bit to 1 creates 13:22:33:FE:44:55:66. If this is used as a part of an IPv6 address it is easy to extract the actual MAC address which then identifies a specific device. See <http://www.tcpipguide.com/free/t_IPv6InterfaceIdentifiersandPhysicalAddressMapping-2.htm> accessed 30 May 2016

[320] Thomas Narten, Richard Draves and Suresh Krishnan, Privacy extensions for stateless address autoconfiguration in IPv6, September 2007, RFC4941 p1 <https://tools.ietf.org/html/rfc4941> accessed 21 January 2017

device at the time the communication was made. However, although there may be no knowledge of a specific user tracking the device across the Internet is made easier with IPv6 even with privacy enabled because the IP address of the device itself, not the home router may be recorded by each server or application that communication is made with.[321] If any personal information in addition to the IP address becomes available to an adversary our actions across multiple websites can become visible and we cannot choose to keep them private.

2.3.6 Internet infrastructure

As was described in the previous section, the Internet consists basically of a whole series of links and interconnections. However, both geography and financial concerns play a large part in defining the overall structure. The principal backbone infrastructure of the Internet is provided by large companies, primarily the large telephone companies which have used their various cable routes to enable large volumes of data to be transmitted. These companies form Tier 1 of a tiered system.

Tier 1 providers, for example AT&T and BT agree to pass Internet data across their networks and between each other at no cost. They interlink Internet Exchange Points (IXPs), large installations that form major intersections in the global Internet. Tier 1 providers also own or lease cables linking countries and continents, typically under oceans. Thus, all of the principal backbone infrastructure of the Internet is provided by Tier 1 companies. Tier 1 companies are also ISPs in their own right. Tier 2 consists of ISPs who connect to IXPs and who will pay for this service. Tier 3 ISPs tend to be local ISPs and in turn get their Internet provision from Tier 2, or in some cases Tier 1 companies.

---

[321] An experiment carried out via Sky broadband showed that three different Apple devices shows three different IPv6 addresses in public when checked with Google's 'what is my IP address' service. None identified the actual device by MAC address suggesting that the privacy extension is activated.

Customers, depending on size can connect to any tier provider. In addition to this are cables held privately by major companies which may also sell Internet bandwidth. A typical home broadband user will connect to a provider at Tier 2 or 3 which in turn will by service from a larger provider. The implications for privacy here are that potentially many companies in many jurisdictions technically can have access to your data while in transit, putting informational privacy at risk.

2.3.6.1 Carrier Grade Network Address Translation

Although IPv6 provides an address space large enough for the planned expansion of the Internet it's uptake has been slow. Because there are few IPv4 addresses left a means had to be found to address the issue. This came in the form of Carrier Grade Network Address Translation (CG-NAT, or CGN).

As shown above, in a home context, NAT means one cannot readily identify the actual person within a property who sent or received a communication. A far more major complication comes with CGN. Unlike NAT used to connect a home network to the Internet where a small number of systems share a common, ISP-allocated public IP address, CGN is implemented within the carrier network itself and connects all users to which that ISP provides access services. It is one mechanism proposed to aid the rollout of IPv6 while the IPv4 addresses are further depleted. Although this breaks the end-to-end model from the early days of the Internet, most home users are already behind a NAT and until, or, indeed, if IPv6 completely replaces IPv4 these techniques are required.[322]

However, CGN provides an issue for Internet surveillance. From a surveillance perspective, depending where one surveils the data, it can be extremely complex to work out the source or destination of a communication from the IP addresses alone as a single IP address may well be used by thousands of simultaneous individual communications potentially sent or

---

[322] Dan Wing, 'Network address translation: extending the Internet address space', IEEE Internet Computing Vol 14 issue 4, July-August 2010, 70

received by thousands of individuals.[323] Therefore, a side effect of the introduction of CGN is the enhancement of Internet privacy.

2.3.7 The Domain Name Service (DNS)

As discussed above, the Internet uses IP addresses to route information between communicating devices. However, humans need a more readable way of accessing information, or to send emails. Email addresses and website addresses share a name component which indicates the resource – be it email address or website – which is to be used. This is termed the *domain name*. The domain name forms a part of a URL and email address. For example, the URL leeds.ac.uk/news has the domain name leeds.ac.uk, as does the email address xyz123@leeds.ac.uk. The Internet uses IP addresses to route information and so a mechanism is used to translate between the domain name and the IP address which will actually be used. This is known as the *Domain Name System* (DNS). Of note, the DNS gives flexibility to Internet addresses in that the IP address need not remain the same. This means that domains can be transferred between ISPs, or may lead to multiple IP addresses for the purpose of resilience.

Although the DNS is necessary in order to make Internet addresses humanly readable there are risks to privacy even here, not because of the basic function of the DNS but by the fact that it can be faked. For example, a user wants to visit a specific website and so they enter the website URL into their browser. The browser causes the underlying system to look up the IP address associated with the URL via the DNS. If the DNS reply can be faked, the user could be diverted to a different website. If that website was convincing enough the user would not be aware of the change and may thus reveal personal information to a fake, rogue website.

---

[323] Chris Donley and others, 'Assessing the impact of NAT444 on network applications, Internet Engineering Task Force', 25 October 2010 <http://tools.ietf.org/html/draft-donley-nat444-impacts-01> accessed 16 February 2013

2.3.8 Internet summary

Several key facts are evident and noteworthy in this research. While the Internet appears simple to the user it is a complex construct of devices and links, defined in part by geography and cost, and by business decisions. The addresses, while unique, cannot indicate who was using any device at any given time. It is often not feasible to assume that any given website is even in the same country as the company that operates it.

There are also weaknesses caused by the complexity and the fact that the Internet has grown from an early academic beginning where security was not a consideration. Weaknesses in the DNS, for example, have been exploited by hackers as well as state actors, and have gained the attention of security services as revealed by the Snowden revelations.

2.4 The growth of the web as a social environment

Two relatively recent phenomena are critical to the modern day use of the Internet. The first phenomenon, the second generation Web (Web2.0) enabled interaction – it enabled people to put data into the Web, not just read information already there. Information input before that time consisted mainly of forms on websites which a person would need to fill in in order to order goods, for instance. After the Web2.0 revolution, anyone could put any information about themselves onto the Web, for example via blogs.[324]

The second phenomenon is described as the semantic web.[325] The driving principle of the semantic web is that data can be accessed not only by humans but also by computer. This gives the ability to re-purpose data in any number

---

[324] Although technically blogs existed well before Web2.0, the expansion of blogging and vastly improved mechanisms to enable blogging became established after Web2.0 had become established.

[325] For further information see <http://www.w3.org/standards/semanticweb/> accessed 4 December 2010

of different ways from any number of different sources. In a sense this has echoes of the worries that first brought about data protection legislation.

There is one important and major development from Web2.0, and this is people's interactions via social media networks.[326] These aim to mimic social structures and can thus import the problems surrounding privacy into cyberspace. The use of social media networks to communicate with friends and family is no different to discussions in the playground, the office or the home. In this respect, the communications channel may be considered similar to e-mail. However, where social media differs is in the way people are required, or at least persuaded to use their personal information to form a profile. This is further examined in Chapter 7.

The 2007 Pew Digital Footprints survey found that one in three adults who publish personal information online in some way have their home address and employer details available.[327] In particular, it was found that '[m]ost internet users are not concerned about the amount of information available about them online, and most do not take steps to limit that information.'[328]

Facebook launched in February 2004 and in September 2016 claimed to have an average of 1.18 billion active users per day.[329] It modelled itself on existing social structures, initially forming groups relating to universities and colleges. It went from 400 million to 500 million active users between February and July

---

[326] Social media networks are taken to mean websites such as Facebook, many of which require the user to lodge personal information before the site can be used effectively.

[327] Pew Internet and American Life Project, 'Digital Footprints: online identity management and search in the age of transparency', December 2007, <http://www.pewinternet.org> accessed 10 January 2011 p16

[328] Ibid., p30

[329] Stats (*Facebook*) <http://newsroom.fb.com/company-info/> accessed 25 January 2017

2010. It knows an ‘immense amount’[330] about its subscribers. Where a Facebook profile is filled in completely, the software records a ‘reasonably comprehensive snapshot’[331] of each person and who they know.[332] Even joining a Facebook group gives information away. For example, becoming a member of some action group indicates not only you are a member, but indicates to others that you are the kind of person who cares about the action in question.[333] One cannot use Facebook to find friends if those friends do not use publish sufficient information to aid your searches. As stated by Westin (Section 2.2 page 21) anonymity is a ‘major aspect of privacy’[334] and one can see from the above that anonymity and Facebook do not go hand in hand.

2.5 The evolving Internet - Internet of Things (IoT) and cloud based services

The Internet as existing from its initial conception has always dealt very simply with the transfer to data from place to place, typically from edge to edge, where client systems and servers are connected at the edge. More lately data may be held on machinery which forms a part of the fabric of the Internet. However, the actual location of data is becoming increasingly blurred by two developments, that of cloud based services, and the Internet of Things. Both of these have different issues for privacy.

---

[330] James Grimmelmann, ‘Facebook and the Social Dynamics of Privacy’ (New York Law School Legal Studies, Research paper series 08/09 #7) p9

[331] Ibid.

[332] Facebook has a concept of 'friends' where people link up to each other. This then becomes a part of the information available to others.

[333] Grimmelmann (n 330) 12

[334] Westin (n 42) 31

2.5.1 Cloud based services

As technology changes so do definitions used to describe it. As the Internet evolves towards more distributed computing and storage facilities, the term ‘cloud’ has become widely used, in particular as ‘cloud storage’ and ‘cloud computing’. Taken in its simplest form, cloud based services are no different from any other Internet service. For example, and email service may be described as cloud based, but technically there is still an email server somewhere which handles the transfer of the email, and there is still some access mechanism used to compose and receive the email. Cloud storage simply means that files are stored on a server somewhere on the Internet.

Technically, then, cloud-based services introduce nothing new as it is simply a way to think of the technology involved. However, there is one significant difference in that with cloud-based services, one can never be sure where one’s data is being held or to where it is being transferred. This has clear implications for privacy, and will become especially relevant and will be further discussed in Chapter 6.

2.5.2 The Internet of Things (IoT)

The Internet of Things (IoT) began life as Machine to Machine (M2M) communications. However, IoT can be considered a superset of M2M because a user’s PC, like everything else on the Internet which can hold or use data can be considered a ‘thing’. IoT is the connection to the Internet of everyday items, not just PCs and servers.

In IoT, household items such as smart TVs, Internet enabled refrigerators and washing machines, security systems and cameras and all such devices can be connected to the Internet. However, IoT is not simply the means by where one can control one’s TV via the Internet; it is about the ability of all these devices to communicate with each other, either with or without a human communications element. It is technically feasible, for example, to construct a refrigerator which uses Radio Frequency ID (RFID) tags on the items inside to determine when an item is removed and replaced, to determine how much of that item is left and to re-order it automatically.

The disadvantage of IoT from a privacy perspective is that one's data can literally be spread anywhere. Unlike cloud services which are typically used either intentionally (if not consciously) or automatically but in a limited way (e.g. sharing data between Internet connected personal devices, phones, tablets, laptops etc.), in IoT, every item of technology one comes across in life may be interconnected and may share data.

2.6 Conclusion

This chapter has examined the meaning of privacy in an Internet context and shown how it is defined and protected both internationally and in the three chosen jurisdictions. It has shown how privacy is a vital right, enabling personal autonomy and liberty and protecting our personal information. From this chapter it is clear that although one can recognise privacy and know what it means on a personal level, being able to define privacy completely in law is impractical. Privacy covers many aspects of our lives yet is not universal. Even defining the meaning of privacy is complex, the matter being made worse by cultural differences.

Additionally, this chapter has investigated the Internet from a technical perspective and this will be built upon in Chapter 6 when the fact that technology can both enhance and invade privacy is discussed. The Internet has been described as 'surveillance-ready'.[335] Every router that the data passes through could conceivably have access to that data, regardless of whether it uses any of it.

While privacy of communications may be achievable via face to face contacts, it is far more difficult to achieve on the Internet. There are two aspects of risk to information privacy on the Internet. First, one's actual communication can be intercepted and thus, no longer remain private between sender and recipient. Second, the mere fact that a communication took place can be recorded. In this respect, the Internet differs dramatically from other forms of

---

[335] John Palfrey, 'The public and the private at the United States border with cyberspace', 78 Miss. L.J. 242 2088-2009, 248

communication. Two people meeting face to face to exchange a written communication may do so in private and unseen. Two people communicating in private across the Internet is closer to two people communicating by shouting at each other across a crowded room.

The next chapter investigates Internet privacy and surveillance from a US perspective in order to evaluate whether or not Internet privacy in the US is dead.

Chapter 3: Internet privacy and communications surveillance in the US

3.1 Introduction

Chapter 2 investigated the meaning of privacy and determined the principal values protected by privacy were autonomy and liberty. It also highlighted that privacy on the Internet is important to protect our personal information. The structure of the Internet was explained in order to provide an understanding of how and where privacy can be lost.

The aim of this chapter is to investigate communications surveillance in the US in order to determine whether or not Internet privacy in the US is dead. It begins with an examination of a wiretapping case from the prohibition era. Wiretapping quickly followed the introduction of the telegraph in the US and continued through changes in technology that brought the telephone. The term is still used today in an Internet context.[336] The technique of wiretapping may have changed but the idea behind it – tapping a communication link to gain access to the data carried across it – remains the same. Therefore, investigating this form of surveillance will form a basis for understanding the issues from an historic perspective and leading to the present day. This is particularly relevant when taking into account the Snowden revelations of 2013.

3.2 Communications surveillance in the USA

One of the first major privacy cases in the US of relevance to this research came about during the Prohibition era and relates to the extensive use of wiretapping in order to combat that crime.[337] The landmark *Olmstead*[338] case

---

[336] Whitfield Diffie and Susan Landau, *Privacy on the Line: The Politics of Wiretapping and Encryption* (MIT Press, Cambridge, 1998), 154-5

[337] Richard C Donnelly, 'Electronic Eavesdropping', 38 Notre Dame L. 667 1962-1963, 668

[338] *Olmstead v. US*, 277 US 438 (1928)

surrounds the unlawful importation of liquors during the Prohibition. Government agents had gathered evidence from wiretaps placed on the telephone lines outside the defendant's property without any need to enter onto the property and without obtaining a warrant. The Court determined that, as there had been no trespass into the property concerned or seizure of any material, the wiretapping did not require a warrant.[339] This was in line with the wording of the Fourth Amendment which itself aimed to protect people from excessive searches by the British in colonial times. However, the case raised several key points. Brandeis J. pointed out that tapping a telephone invades not only the privacy of the subscriber but also that of 'every other person'[340] who calls the subscriber or who the subscriber calls. Fisher suggests the Court was 'thrown off balance by a technological development that did not fit conventional legal arguments'.[341] Holmes J. stated that it was 'less evil that some criminals should escape than that the government should play an ignoble part.'[342] These points, made over 60 years before the invention of the Web still hold true today where an Internet tap even at a small ISP can give access to the communications of thousands of people, none of which may be under any suspicion.

Communications privacy received attention six years later. A single section in the Communications Act of 1934.[343] Section 605[344] of the Act made it illegal for anyone involved in the carrying of communications to divulge or publish the contents or even the existence of those communications. However, the Justice Department took the view that s.605 only prevented the divulgence of

---

[339] David Barnum, 'Warrantless electronic surveillance in national security cases: lessons from America', E.H.R.L.R 514, 2006, 519-520

[340] Olmstead (n 338) 476

[341] Louis Fisher, 'Congress and the fourth amendment', 21 Ga. L. Rev. 107 1986-1987, 125

[342] Olmstead (n 338) 470

[343] Communications Act of 1934, 47 USC S151 et seq.

[344] Ibid., s.605

material gained via wiretapping rather than ruling out wiretapping *per se* and that only when material is passed outside of the government does it then become divulgence.[345] Because of this loophole, wiretaps continued to be used in criminal investigations until important Supreme Court rulings in 1937.[346] These rulings related to an alcohol smuggling case which met the appeals court twice.

Nardone *et al* had been convicted of smuggling alcohol. In the first *Nardone v United States*,[347] the court concluded that s.605 clearly prohibited the use of intercept material.[348] Convicted again, in the second *Nardone v United States*[349] case, the court affirmed that not only was the product of an illegal wiretap inadmissible as evidence, any evidence gained by the use of the wiretap material could not itself be used.[350] In addition, in *Weiss v United States*,[351] the court ruled that s.605 applied to intrastate communication as well as interstate communications. However, what should have been a positive outcome for communications privacy only resulted in wiretap evidence not being used in court rather than not being used at all.[352]

---

[345] Wayne R LaFave, Jerold H Israel and Nancy J King, *Criminal Procedure (3rd edn.)* (West Group, Minnesota, 2000), 260

[346] Kimberley A Horn, 'Privacy versus protection: exploring the boundaries of electronic surveillance in the Internet age', 29 Fordham Urb. L. J. 2001-2002, 2239

[347] *Nardone v United States* 302 US 379 (1937)

[348] Ibid., 382

[349] *Nardone v United States* 308 US 338 (1939)

[350] Ibid., 340 to 341

[351] *Weiss v United States* 308 US 321 (1939)

[352] United States Senate, *Final Report of the Select Committee to Study Governmental Operations with respect to Intelligence Activities: Book III: Supplementary Detailed Staff Reports on Intelligence Activities and the Rights of Americans* (US Government Printing Office, Washington, 1976), 278-279

The *Olmstead* ruling regarding physical entry saw the government succeed in *Goldman v United States* where a device had been used to listen through a wall adjoining the defendants property with no trespass.[353] Access to a workplace was not considered trespass in *On Lee v United States*[354] where an agent used an electronic bug so that agents outside could hear On Lee make self-incriminating statements.[355] However, the Court upheld the warrant requirement for physical entry when in *Silverman v United States*,[356] a microphone had been pushed into the defendant's house.[357]

So far, it is evident that physical intrusion into someone's privacy was required in order for a warrant to be necessary. Had this remained the case, it would be clear that surveillance would go unchecked by the courts because the necessary infrastructure must pass out of the private space and thus become accessible for tapping. Despite this, one key case, *Katz v United States.*[358] reversed the *Olmstead* view and brought electronic surveillance firmly within the reach of the Fourth Amendment. This is discussed next.

3.2.1 The introduction of warrant requirements

The *Olmstead* doctrine was finally reversed in *Katz* who had been convicted of passing betting information across US state lines, violating 18 USC S1084. The FBI had used an electronic recording device outside the telephone booth that Katz used for his trade. On appeal, the conviction was upheld, agreeing with the *Olmstead* doctrine that there had been no physical intrusion and therefore no Fourth Amendment violation. The case progressed to the Supreme Court which reversed *Olmstead* and found that the Fourth

---

[353] *Goldman v United States* 316 US 129 (1942)

[354] *On Lee v United States* 343 US 747 (1952)

[355] Ibid., 751-752

[356] *Silverman v United States* 365 US 505 (1961)

[357] Ibid., 509

[358] *Katz v United States* 389 US 347 (1967)

Amendment 'protects people, not places'[359] and that whatever a person 'seeks to preserve as private, even if in an area accessible to the public, may be constitutionally protected'.[360] The Court found that the Government's activities in this case constituted a search and seizure. In his concurring opinion Harlan J. outlined what became a well-established test: a person must have an actual expectation of privacy, and society itself must regard that expectation as reasonable,[361] tying privacy to social norms. If this test is met, a person thus has a 'constitutionally protected reasonable expectation of privacy'.[362]

The *Katz* judgement 'represented a paradigm shift in Fourth Amendment analysis.'[363] The clarification in *Katz* that electronic eavesdropping constitutes a search or seizure and that searches and seizures do not require physical trespass or confiscation represented a change in the way courts would view the privacy protections offered by the Fourth Amendment.[364] However, the *Katz* court carefully avoided the national security question.

The procession of cases from *Olmstead* to *Katz* have evidently shown how the law is continually being left behind by advances in technology and how agencies will attempt to justify their actions by lose reading of the relevant law. However, Congress was by now catching up on the issue of privacy and wiretapping was included in the Omnibus Crime Control and Safe Streets Act (OCCSSA) of 1968. Congress recognised that there had been extensive illegal wiretapping in the past and they needed to find a way to protect the privacy of communications while still permitting law enforcement to carry out

---

[359] Ibid., 351

[360] Ibid.

[361] Ibid., 361

[362] Ibid., 360

[363] Timothy Casey, 'Electronic surveillance and the right to be secure', 41 UC Davis L. R. 3, 2008, 979

[364] David Sklansky, 'Back to the future: *Kyllo*, *Katz* and common law', 72 Miss. L. J. 143 2002-2003, p153-154; see also 407 US 297 at 302

interceptions.[365] Title III of the Act deals with wiretaps and its major purpose was to deal with organised crime, finally requiring the courts to authorise wiretapping via warrants. Furthermore, it set surveillance as the exception, not the rule - a condition when seeking a warrant was that other investigative methods had been attempted.[366]

However, once again, the national security question was avoided, the Act including a clause stating that neither it nor s.605 of the Communications Act of 1934 limited the constitutional power of the President 'to take such measures as he deems necessary'[367] in order to protect the US. This included that the contents of intercepted communications gathered under the authority of the President granted by this section of the Act could be used in evidence. This was subsequently relied upon by the Executive as permitting electronic surveillance for purposes of national security but would soon be tested in the courts and this is examined next.

3.2.2 Strengthening warrant requirements

In *United States v United States District Court*[368] (also known as *Keith*[369]), a warrantless wiretapping case in 1972, the Court held that the constitutional power of the President did not extend to the authorisation of warrantless electronic surveillance in domestic security cases. Maclin describes the case as a 'more constitutionally robust and stronger version of *Katz*'.[370] The Government claimed exemption from the warrant requirements of the Fourth

---

[365] Omnibus Crime Control and Safe Streets, Pub. L. No. 90-351, 82. Stat. 197, (OCCSSA) Title III Findings

[366] Ibid., 2518 (1)(c)

[367] Ibid., 2511 (3)

[368] *United States v United States District Court* 407 US 297 (1972)

[369] The name Keith refers to the then US District Court Judge Damon Keith.

[370] Tracey Maclin, 'The Bush administration's terrorist surveillance program and the Fourth Amendment's warrant requirement: lessons from Justice Powell and the *Keith* case', 41 U.C. Davis L. Rev. 1262 2007-2008, p1263

Amendment, claiming it to be a 'reasonable exercise of presidential power to protect the national security.'[371] Before the trial, the defendants had attempted to obtain the evidence. The Government refused, but the District Court held that the wiretaps violated the Fourth Amendment and ordered the evidence to be produced. In response to this, the Government appealed to the Court of Appeals for the Sixth Circuit to set aside the judgment of the District Court. The Court of Appeals determined that the District Court had been correct in its judgment and the case progressed to the Supreme Court.[372] Delivering the opinion of the Court, Powell J. stated that the case required 'sensitivity both to the Government's right to protect itself from unlawful subversion and attack and to the citizen's right to be secure in his privacy against unreasonable Government intrusion.'[373]

The Government relied on the proviso in Title III regarding the constitutional powers of the President[374] to determine that this includes warrantless wiretaps in domestic security cases. The Court disagreed, arguing that Section 2511(3) of Title III does not confer any powers on the President and was written so as to not interfere with any powers the President had already as defined in the Constitution.[375] The requirement for warrants under Title III was clear and the Court affirmed the findings of the Court of Appeal. Douglas J. pointed out that if warrants were not required, it would mean that the US intelligence agencies would 'literally enjoy unchecked discretion',[376] able to sift through every telephone conversation and seize those few words which might 'add to their sense of the pulse of a domestic underground.'[377] The 2013 Snowden

---

[371] Ibid.

[372] Ibid., 300-301

[373] Ibid., 298

[374] OCCSSA (n 377) 2511 (3)

[375] United States v United States District Court (n 368) 303

[376] Ibid., 325

[377] Ibid., 325

revelations which are covered in Chapter 6 suggest that this is exactly what was put into place with regard to Internet surveillance.

The Court was careful to state that it was only considering the domestic issue and had no opinion with regard to surveillance of the activities of foreign agents or powers.[378] It did invite Congress to consider the matter of foreign intelligence, going as far as to suggest that different protective standards may still be acceptable under the Fourth Amendment. After six years of 'debate, compromise, and negotiation'[379] between those agencies who wished to carry out surveillance and the legislators who wanted a warrant requirement and taking into account the excesses of the Executive in the Watergate scandal[380] Congress passed the Foreign Intelligence Surveillance Act of 1978 (FISA).[381]

3.3 The Foreign Intelligence Surveillance Act of 1978

FISA was preceded by two Executive Orders which set out to regulate surveillance. Executive Order 11905 (EO11905)[382] required that surveillance should be conducted with due respect to privacy and civil liberties. It also banned unlawful interception of communications sent from or to the US or destined for a US person located abroad. The order was superseded by

---

[378] United States v United States District Court (n 368) 321-322

[379] Alison A Bradley, 'Extremism in the defense of liberty?: the Foreign Intelligence Surveillance Act and the significance of the USA PATRIOT Act', 77 Tul. L. Rev. 465 2002-2003, 473

[380] Susan Landau, *Surveillance or Security? The Risks Posed by New Wiretapping Technologies* (The MIT Press, Cambridge, 2010), 76; The Watergate scandal is an example of the abuse of executive power in the US. What began with a burglary at the offices of the Democratic National Committee led to the discovery of illegal activities by the Nixon administration including communications surveillance. It resulted in the resignation of President Nixon who was by then facing impeachment.

[381] Foreign Intelligence Surveillance Act of 1978 (Pub. L. 95–511, 92 Stat. 1783, 50 USC Ch. 36)

[382] Executive Order 11905, 41 Fed. Reg. 7703 (Feb 18, 1976)

Executive Order 12036 (EO12036)[383] which required the use of the least invasive means possible when gathering intelligence. This order also required that there be probable cause to believe a targeted US person located abroad was an agent of a foreign power.[384]

FISA provides the President with substantial powers to conduct surveillance for foreign intelligence purposes. 'Notwithstanding any other law',[385] electronic surveillance can be authorised for up to one year without a court order, certified only by the Attorney General that the targets are foreign powers or premises thereof,[386] that there is 'no substantial likelihood'[387] that the surveillance would acquire communications to which a US person is a party, and that there is an adequate minimization procedure.[388]

FISA also provides for surveillance under court order. Applications for court orders under FISA require that the purpose of the surveillance is to obtain foreign intelligence,[389] and that the information cannot be obtained by other more normal investigations.[390] Such orders are issued by the Foreign Intelligence Surveillance Court[391] (FISC) which Robinson states is a secret court 'accountable only to itself',[392] its work hidden from public view and

---

[383] Executive Order 12036, 43 Fed. Reg. 3674 (Jan 24, 1978)

[384] Jonathan Gannon, 'From Executive Order to Judicial Approval: Tracing the History of Surveillance of U.S. Persons Abroad in Light of Recent Terrorism Investigations', 6 J. Nat'l Sec. L. & Pol'y 59 2012, 71

[385] 50 USC S1801(a)(1)

[386] 50 USC S1801(a)(1)(A)

[387] 50 USC S1801(a)(1)(B)

[388] 50 USC S1801(a)(1)(C)

[389] 50 USC S1804(a)(7)(B) as originally codified

[390] 50 USC S1804(a)(7)(C)

[391] 50 USC 1803

[392] Gerald H Robinson, 'We're listening! Electronic eavesdropping, FISA, and the secret court', 36 Willamette L.Rev. 51 2000 at p51

unaccountable, all in the name of national security.[393] 'Probable cause' is handled differently in FISA which does not require ‘individualized suspicion of criminal activity’.[394] Provided the surveillance target is a ‘foreign power or an agent’[395] thereof and the place which will be surveilled is being used by or will be used by the target,[396] an order for surveillance will be granted. A major criticism of FISA is that a warrant can be issued ‘without probable cause that a crime has been or will be committed’,[397] the test in FISA being only that the target is believed to be a foreign power or agent thereof, or the premises is believed to be used by a foreign power or agent thereof.[398] Meason argues that FISA ‘came into being as much to facilitate surveillance as it did to prevent its abuse’.[399] However, Blum argues that the difference in probable cause tests indicates the difference between surveillance for preventative intelligence gathering under FISA vs surveillance to gather evidence of crime.[400]

The language of FISA is ‘vague and subject to elastic interpretation.’[401] FISAs principal target definitions are foreign powers or agents of foreign powers. Nevertheless, this research finds that exactly what constitutes each is

---

[393] Ibid., 54

[394] Gregory Birkenstock, ‘The Foreign Intelligence Surveillance Act and standards of probable cause: an alternative analysis’, 80 Georgetown L. Rev. 843 (1992) p851

[395] 50 USC S1804 (a)(4)(A)

[396] 50 USC S1804 (a)(4)(B)

[397] Birkenstock (n 394) 851

[398] 50 USC 1805(a)(3)(A) and (B) (2000)

[399] James E Meason, ‘The Foreign Intelligence Surveillance Act: time for reappraisal?’, 24 Int'l L 1043 (1990) at 1047

[400] Stephanie Cooper Blum, ‘What really is at stake with the FISA Amendments Act of 2008 and ideas for future surveillance reform’, 18 B.U. Pub. Int. L. J. 269 2008-2009, 276

[401] Robinson (n 392) 56

subjective. A foreign government or part thereof is clearly a foreign power.[402] Less clear is a 'faction of a foreign nation or nations, not substantially composed of United States persons.'[403] For instance, Robinson questions how one enumerates the term *substantial* and suggests that FISC simply decides for itself.[404] Terrorist groups,[405] foreign-based political organisations,[406] and entities directed and controlled by foreign governments[407] are also classed as foreign powers.

FISA contains a primary purpose test to ensure that it is used to acquire foreign intelligence. Where any information gained is to be used in a criminal prosecution FISA contains the safeguard that any such information must first be made available to the person concerned.[408] This safeguard permits that person to submit motions to suppress the information.[409] This primary purpose test was established in *US v Truong*,[410] a case involving surveillance in 1977 before FISA was enacted. The district court had accepted that there was a foreign intelligence exception to the requirement for a warrant but that this existed only where the investigation was primarily one concerning foreign intelligence. The court of appeal agreed that 'courts are unschooled in

---

[402] 50 USC S1801(a)(1)

[403] 50 USC S1801(a)(2)

[404] Robinson (n 392) 56

[405] 50 USC S1801(a)(4)

[406] 50 USC S1801(a)(5)

[407] 50 USC S1801(a)(3) and (6), the wording is broadly similar

[408] Foreign Intelligence Surveillance Act of 1978 S106(c) and (d), 50 USC S1806(c) and (d) (2000)

[409] Foreign Intelligence Surveillance Act of 1978 S106(e), 50 USC S1806(e) (2000)

[410] 629 F.2d 908, United States of America, Appellee, v. Truong Ding Hung, Appellant. United States of America, Appellee, v. Ronald Louis Humphrey, Appellant.

diplomacy and military affairs'[411] and thus not competent to judge whether or not a foreign intelligence warrant request should be granted. However, the court stressed that where an investigation becomes primarily a criminal one, the courts are 'entirely competent'[412] and therefore a warrant requirement exists.

3.4 Privacy in communications data given voluntarily

Fourth Amendment protection does not apply where information has been given voluntarily to third parties and this was highlighted in *Smith v Maryland.*[413] In this particular case, evidence from a pen register which had been installed without a warrant was used to gain a search warrant for Smith's residence. Smith argued that, because there was no warrant for the pen register any evidence gained as a result should be excluded. However, the appeals court determined that there is no expectation of privacy with regard to numbers dialled into the telephone system and thus no warrant was required.[414] Telephone subscribers as a whole must realise the need to send numbers to the telephone company in order to make a call. Moreover, subscribers must also realise that the telephone company can see these numbers should they need to, on one hand for billing purposes, and on the other to trace obscene phone calls, a fact highlighted in the customer information pages of many telephone directories. Therefore, applying *Katz*, Smith's expectation of privacy is not reasonable and thus fails.[415] In effect it means there is no privacy in the specific communications metadata – phone numbers – as these are voluntarily turned over to a third party.[416] This became

---

[411] Ibid., at 14

[412] Ibid., at 19

[413] 442 US 735 (1979)

[414] 442 US 735 at 738

[415] 442 US 735 at 742 - 744

[416] 422 US 735 at 743

known as the Third Party Doctrine and would come to permit the bulk Internet metadata collection revealed by Snowden (as discussed in Chapter 6).

However, the decision was not unanimous. In his dissenting statement, Stewart J. considered that dialled numbers should gain Fourth Amendment protection because a list of such numbers 'could reveal the identities of the persons and the places called, and thus reveal the most intimate details of a person's life.'[417] Although it dealt with telephone numbers, this statement is particularly relevant when applied to the Internet privacy and the use of metadata as will become evident in Chapter 6.

3.5 Executive Order 12333: Expanding FISAs reach

FISA did not govern the surveillance of US persons who were located outside of the US. This was addressed in 1981 by Executive Order 12333 (EO12333)[418] which was issued by the President on 4th December 1981 and superseded EO12036. This order specified that the 'least intrusive collection techniques feasible'[419] be used within the US or targeting a US person abroad, echoing the provisions of EO12036. Permission to target a US person either in the US or abroad would be granted by the Attorney General with the specific requirement that electronic surveillance must be conducted in accordance with both FISA and EO12333.[420]

Although written in 1981 and amended several times, the sections outlined above remain intact and relevant to Internet surveillance.[421] EO12333 would

---

[417] 442 US 735 at 748

[418] Executive Order 12333, 46 Fed. Reg. 59941 (Dec 4, 1981)

[419] Ibid., 2.4

[420] Ibid., 2.5

[421] EO12333 was amended by Executive Orders 13284 (2003), 13355 (2004) and 13470 (2008)

become key to the NSA's activities described in the Snowden revelations of 2013 and this is discussed in more detail in Chapter 6.

3.6 The Electronic Communications Privacy Act

This research also finds that the wording of OCCSSA Title III and therefore the privacy protection it offered in a changing technological landscape did not stand the test of time. One principal issue was that Title III only considered aural communications and therefore, it offered no protection for digital modes. Put simply, the application of the Fourth Amendment had not kept up with advancing technology.[422]

On 21st October 1986, the Electronic Communications Privacy Act of 1986[423] (ECPA) was signed into law. Of particular note during discussions at the Bill stage, Senator Leahy pointed out that it is not the rules but the technology that changes, legislation ensuring that the rules keep pace with the technology.[424] This remains true today and had earlier Acts considered this, there may have been fewer issues in the past.

ECPA amended Title III of OCCSSA to cover intercepts of electronic communications.[425] It divided electronic communications into three sections,

---

[422] Federal Government Information Technology: Electronic Surveillance and Civil Liberties (Washington CD, US Congress, Office of Technology Assessment, OTA-CIT-293, October, 1985) <http://www.justice.gov/sites/default/files/jmd/legacy/2013/10/15/fgit-1985.pdf> accessed 17 December 2015

[423] Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848

[424] Senator Leahy, Hearings before the subcommittee on courts, civil liberties, and the administration of justice of the committee on the judiciary, house of representatives, 99th Congress, 1st and 2nd sessions, on H.R.3378 Electronic Communications Privacy Act, p18 <http://www.justice.gov/jmd/ls/legislative_histories/pl99-508/hear-50-1985.pdf> accessed 29 June 2014

[425] 18 USC S2510(4) as amended

namely the Wiretap Act,[426] the Stored Communications Act (SCA)[427] and the regulation of pen registers and trap and trace devices.[428] The warrant requirements of Title III remained unaffected.

ECPA set in place the requirement that communications information could not be obtained without the customer's permission unless it was done so via a court order or warrant. The exception to this was the National Security Letter (NSL).[429] The ECPA enabled the FBI issue a NSL to obtain subscriber information including metadata. In order to use a NSL the FBI had to certify that the information sought was in conjunction with a foreign intelligence investigation. Because of this, the authority of a NSL was less than that of a subpoena but was 'perfectly sufficient in situations where state privacy legislation presented the only barrier to compliance'.[430]

3.6.1 The Stored Communications Act

Title II of the ECPA is known as the Stored Communications Act (SCA)[431]. Described by Kerr as 'dense and confusing',[432] its aim is to regulate access to both the content of communications in electronic storage and access to subscriber information. Unlike wiretaps, which can only give access to information passing across the tap from the day the tap was installed going

---

[426] 18 USC S2510 – 2522

[427] 18 USC S2701 – 2712

[428] 18 USC S3121 – 3127

[429] Brett A Shumate, 'Thou shalt not speak: the nondisclosure provisions of the National Security Letter statutes and the First Amendment challenge', 41 Gonz. L. Rev 151 2005-2006 p154

[430] Andrew E Neiland, 'National Security Letters and the amended Patriot Act', 92 Cornell L. Rev. 1201 2006-2007, 1210

[431] Stored Communications Act, 18 USC Ch. 121 S2701-2712

[432] Orin Kerr, 'A user's guide to the Stored Communications Act, and a legislator's guide to amending it', 72 Geo. Wash. L. Rev 1208 2003-2004 p1208

forward, the SCA gives access to data already held on computers and this would include e-mails stored at an ISP, for instance.

Regarding the content of any communication stored by the ISP the SCA sets a 180 day limit within which the government can only gain access pursuant to a warrant.[433] However, where a communication had been stored for more than 180 days, the government only needs a court order and for this, it only needs to show 'reasonable grounds'[434] to believe the material requested is relevant to an on-going criminal investigation. This is less than the probable cause requirements for a warrant and Cady notes that this falls short of the standard required by the Fourth Amendment.[435] This issue was dealt with by the Court of Appeal and is examined next.

3.6.2 *Warshak*, a challenge to the SCA grant of access to e-mails

Warshak consists of a series of cases surrounding fraud and money laundering. It saw the US Court of Appeals for the 6th Circuit become the first Article III court to address the question of whether someone has a reasonable expectation of privacy with regard to emails stored on a third-party server.[436] Kerr initially described the first Warshak case[437] as 'a rather odd case involving e-mail privacy'[438] as he did not believe the court would get involved in the technologies. Two months later, he determined that the court had

---

[433] 18 USC S2703(a)

[434] 18 USC S2703(d)

[435] Spencer S Cady, 'Reconciling privacy with progress: Fourth Amendment protection of e-mail stored with and sent through a third-party Internet service provider', 61 Drake L. Rev. 225 2012-2013, 240-241

[436] Ibid., 242

[437] *Warshak v United States* 490 F.3d 455 (2007)

[438] Orin Kerr, The Volokh Conspiracy archive, 17/04/07 <www.volokh.com/posts/1176832897.shtml> accessed 26 January 2014

actually reached a 'blockbuster decision'.[439] That decision, and its implications are discussed below.

Warshak was under investigation for fraud and the government used the SCA to order his ISP to preserve and then to produce his e-mails. Warshak was not made aware of this until over a year after the order had been issued.[440] When he became aware of the action he filed a claim for injunctive relief and a judgement against the US, claiming that the compelled warrantless disclosure of his e-mails constituted a violation of the Fourth Amendment.[441] The District Court found in Warshak's favour and the government appealed. The Court of Appeals for the 6th Circuit affirmed the findings of the District Court and confirmed that Warshak had a reasonable expectation of privacy in his e-mails stored at his ISPs.[442] However, shortly after this decision, the 6th Circuit Court en banc vacated its earlier decision, stating that Warshak's constitutional claim was 'not ripe for judicial resolution.'[443]

The same issue returned to the same court in 2010 when Warshak brought a criminal appeal following his conviction. The Court once again held that by compelling his ISP to turn over 27,000 of his e-mails, the government had violated Warshak's Fourth Amendment rights.[444] The Court applied the Katz test, determining that Warshak had clearly demonstrated an expectation that the privacy of his e-mails would not be interfered with.[445] This satisfied the first prong of the Katz test. The Court then turned to the issue of whether society would consider the expectation of privacy to be a reasonable one, the second

---

[439] Orin Kerr, The Volokh Conspiracy archive, 18/06/07 <www.volokh.com/posts/1182181742.shtml> accessed 26 January 2014

[440] 490 F.3d 455 (n 480) at 460-461

[441] Ibid., 461

[442] Ibid., 473

[443] *Warshak v United States* 532 F.3d 521(6th Cir. 2008)

[444] *United States v Warshak* 631 F.3d 266 (6th Cir. 2010) at 282

[445] Ibid., 284

prong of the Katz test. Here, it determined that because e-mails are fundamentally similar to more traditional forms of communication, clearly they deserve the same protection under the Fourth Amendment.[446] Therefore, the government must obtain a warrant based on probable cause in order to force an ISP to deliver people's e-mails and because the SCA permits the government to obtain e-mails without such a warrant, it declared the SCA to be unconstitutional.[447]

Warshak highlighted the disparity between the protection afforded to letters on the one hand and e-mail on the other. Privacy of communications via postal services is protected as determined in *ex parte Jackson*[448] in 1878. However, the SCA as worded does not translate such protections towards stored e-mail. In declaring the SCA to be unconstitutional, the Court sent a clear signal that e-mail must be afforded the same levels of protection as the more traditional or older forms of communication. As highlighted by Perry it is vital that Fourth Amendment jurisprudence keeps pace with changing technologies - even though e-mail did not exist at the time, the dissenting statement of Brandies J. in *Olmstead* still holds true.[449]

3.7 The Communications Assistance for Law Enforcement Act (CALEA)

Although Title III of the OCCSSA enabled legal wiretaps, it did not provide any means by where law enforcement could coerce telecommunications providers into assisting in investigations.[450] ECPA had amended Title III to bring it in line

---

[446] Ibid., 285-286

[447] Ibid., 288

[448] *Ex parte Jackson* 96 US 727 (1878)

[449] Casey Perry, 'U.S. v Warshak: will Fourth Amendment protection be delivered to your inbox?', 12 N.C. J.L. & Tech. 345 2010-2011, 367

[450] Hildegarde A Senseney, 'Interpreting the Communications Assistance for Law Enforcement Act of 1994: the Justice Department versus the

with technology which was new at that time, but the legislation was not future proof.[451] In particular, the change to digital and mobile communications meant that there was often no wire to attach a wiretap to, and even if there were the digital nature of communications could render them inaccessible. Through several bill proposals,[452] one of which spurred Phil Zimmerman to publish his Pretty Good Privacy (PGP) email encryption code for free,[453] this problem of access would eventually be passed to equipment manufacturers as a requirement to provide such access. This requirement was enshrined in the Communications Assistance for Law Enforcement Act (CALEA) which passed into law in October 1994.

The aim of CALEA is to ensure that CSPs maintain the ability for law enforcement agencies to 'readily install wiretaps on individuals under criminal investigation'[454] in an ever changing environment. CALEA was a major change. Before the Act, wiretap law focused on what could be obtained and how it should be obtained, given the constraints of the technology. CALEA would now effectively dictate how CSPs would configure their networks.[455] In effect, the government would require the telecommunications industry to

---

Telecommunications industry & privacy rights advocates'(1998) 20 Hastings Comm/Ent L.J. 665, 682

[451] David Ward 'Sisyphean circles: the Communications Assistance for Law Enforcement Act' (1996) 22 Rutgers Computer & Technology L.J. 267, 269

[452] See for example Senate Bill S.266 (1991) Comprehensive Counter-Terrorism Act of 1991 s.2201; FBI Digital Telephony Bill sec. 2(a) <https://w2.eff.org/Privacy/Surveillance/CALEA/digtel92_bill.draft> accessed 25 May 2014

[453] Phil Zimmerman, Why I wrote PGP <http://www.philzimmermann.com/EN/essays/index.html> accessed 25 May 2014

[454] Gene D Park, 'Internet wiretaps: applying the Communications Assistance for Law Enforcement Act to broadband services', 2 ISJLP 5990 2005-2006 at 605

[455] Susan Landau, 'National security on the line', 4 J. Telecomm. & High Tech. L. 409 2005-2008, 417

change its products so that the government could better spy on their customers.[456]

3.8 9/11 and the USA PATRIOT Act

On 11th September 2001, members of the terrorist organisation al Qaeda hijacked four commercial aircraft within the US. Two were flown into the twin towers of the World Trade Center in New York, causing both towers to collapse. A third plane hit the Pentagon and the fourth came down in fields without reaching its intended target which was possibly the White House or the Capitol building in Washington DC.[457] This event is popularly known as 9/11. In the wake of the atrocity, thoughts of privacy took a back seat, surveillance gaining increased public support and Congress enacting legislation to increase the authority to surveil[458] in the form of the Patriot Act[459] which became law on 26th October 2001.

Before the Patriot Act, the sole purpose of FISA court orders for surveillance had to be to obtain foreign intelligence.[460] This was weakened such that orders could be obtained where 'a significant purpose'[461] was the acquisition of such foreign intelligence. Not only did this remove the primary purpose standard of

---

[456] Lillian R BeVier 'The Communications Assistance for Law Enforcement Act of 1994: a surprising sequel to the break up of AT&T' 51 Stanford L. Rev. 1049 p1091-92

[457] The 9/11 Commission Report pp4-14

[458] Marc Rotenberg, 'Privacy and Secrecy after September 11', 86 Minn. L. Rev. 1115 2001-2002

[459] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001, PL 107-56, October 26, 2001

[460] 50 USC S1804(a)(7)(B) and 50 USC S1823(a)(7)(B) – see US Code 2000 main edition (2/1/2001)

[461] Patriot Act s.218, codified at 50 USC 1804(a)(7)(B) and 50 USC S1823(a)(7)(B) – see US Code 2000 ed. and supplement 1 (22/1/2002)

FISA[462] but it also posed a real danger that surveillance could be carried out for criminal investigations without the usual warrant requirements.

The scope of FISA was further widened by Section 215 which enabled access to business records about any non-US person or anyone (US people included) if the purpose was to 'protect against international terrorism or clandestine intelligence activities'.[463] The only caveat here is that if the target is a US person, the reason for the investigation must not be *solely* based on activities which attract First Amendment protection.[464] The actual information which may be obtained was greatly expanded, now being termed 'any tangible things'.[465] Section 215 featured heavily in the 2013 Snowden revelations.[466]

Section 216 modified the definition of the recording ability of pen registers and trap and trace devices to include not only dialling information, but also routing and addressing information.[467] This means that these devices can now record IP addresses.

---

[462] Bradley (n 379) 486

[463] 50 USC S1861(a)(1) (see US Code 2000 ed. and supplement 1, 22/1/2002)

[464] 50 USC S1861(a)(1) and 50 USC S1861(a)(2)(B) (see US Code 2000 ed. and supplement 1, 22/1/2002)

[465] 50 USC S1861(a)(1) (see US Code 2000 ed. and supplement 1, 22/1/2002)

[466] Privacy and Civil Liberties Oversight Board, Report on the Telephone Record Program Conducted under Section 215 of the USA PATRIOT Act and on the Operations of the Foreign Intelligence Surveillance Court, 23 January 2014, <https://fas.org/irp/offdocs/pclob-215.pdf> accessed 23 January 2017

[467] 18 USC S3121 General prohibition on pen register and trap and trace device use; exception at S3121(c); see also definitions 18 USC S3127(3) and (4) (see US Code 2000 ed. and supplement 1, 22/1/2002)

3.8.1 Expanding surveillance capabilities

FISA was modified in 2004 by the Intelligence Reform and Terrorism Protection Act of 2004[468] which solved a problem that became apparent after 9/11. The modification altered FISA's definition of an agent of a foreign power to include any non-US person who 'engages in international terrorism or activities in preparation thereof'.[469] This became known as the 'lone wolf amendment'.[470] The FBI had arrested Zacarias Moussaoui on 16 August 2001 after he had sought flight training but with neither the relevant qualifications nor the desire to become a commercial pilot. Moussaoui did not agree for his laptop to be searched. The FBI attempted to assemble a case for a FISA order, but found no evidence that Moussaoui was a member of any terrorist group and were thus defeated by the wording of 50 USC S1801(b) as written at that time.[471]

One may consider the modification for FISA a reasonable one given the changing nature of terrorism. However, the Press would reveal a far more sinister program instigated by the President in the aftermath of 9/11. Despite assurances that wiretapping is not aimed at terrorists without a court order,[472] in December 2005, the New York Times revealed the President signed an order in October 2001 directing the NSA to collect foreign intelligence by the use of electronic surveillance aimed at countering terrorism in the US.[473] The

---

[468] Intelligence Reform and Terrorism Protection Act of 2004, Pub. L. 108-458, 118 Stat. 3638, December 17, 2004

[469] 50 USC S1801(b)(1)(C) (2000 & Supp.V 2006)

[470] S Rep. No. 108-40, at 2, 11 (2003)

[471] Patricia L Bellia, 'The "Lone Wolf" Amendment and the Future of Foreign Intelligence Surveillance Law', 50 Vill. L. Rev. 425 2005, 427-428

[472] 40 Weekly Compilation of Presidential Documents 641, April 20 2004 <http://www.gpo.gov/fdsys/pkg/WCPD-2004-04-26/pdf/WCPD-2004-04-26-Pg638.pdf> accessed 15 September 2014

[473] James Risen and Eric Lichtblau, 'Bush lets U.S. spy on callers without courts', (*New York Times*, 16 December 2005) <http://www.nytimes.com/2005/12/16/politics/16program.html> accessed 22 June 2014. The New York Times had delayed the publication of the

order permitted surveillance in the US without either warrant or court order. Under the Order, the NSA was to collect the contents of international communications under a program later named the Terrorist Surveillance Program (TSP) and to collect bulk telephone and Internet metadata. The authorisation was renewed continually every 30 to 60 days and the TSP and metadata collection became collectively known as the President's Surveillance Program (PSP).[474]

The PSP had none of the safeguards of FISA and provided the intelligence community with powers which were never granted by Congress or the courts.[475] The overall legality of the program was assumed under both Article II of the Constitution and the Authority for Use of Military Force (AUMF)[476] which gave the President broad powers in the fight against terrorism.[477] NSA Director Hayden stated the NSA could not use FISA because obtaining orders via the FISC took too long, and even the emergency provision of 72 hours surveillance before a court order was obtained was not instant, requiring the Attorney General to first ensure the surveillance would in fact be acceptable to the FISC.[478]

---

article by a year after discussion with the White House. Note the article claims the order was signed in 2002 but official documentation released later states October 2001.

[474] Privacy and Civil liberties Oversight Board, Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act, July 2, 2014, p16

[475] Emily Arthur Cardy, 'The Unconstitutionality of the Protect America Act of 2007', 18 B.U. Pub. Int. L. J.171 2008-2009, 174

[476] Authorization for Use of Military Force, Pub L. 107-40, 115 Stat. 224, Sept 18, 2001

[477] Office of Inspectors General, Report on the President's Surveillance Program, Volume 1 , 10 July 2009, p9 <https://oig.justice.gov/reports/2015/PSP-09-18-15-vol-I.pdf> accessed 20 December 2015

[478] Ibid., 6

The TSP finally came to an end on 17 January 2007 when Attorney General Gonzales informed the Senate that the TSP would not be reauthorised. The reason was that the FISC had issued orders which authorised the Government to surveil communications into and out of the US where it believed that one of the parties was a member of al Qaeda or an associated organisation.[479]

FISA was once again modified by the Protect America Act of 2007 (PAA)[480] which redefined the meaning of electronic surveillance under FISA such that it excludes any surveillance of a person 'reasonably believed to be outside of the United States.'[481] This effectively removed all of the protections provided by FISA as well as any limitation that FISA placed on collection methods or scope where the target is outside the US.[482] In other words, it permitted warrantless surveillance of communications between foreign people outside the US where those communications happened to be routed through the US.[483] The significance for Internet privacy is that a great deal of the world's Internet traffic may be routed through the US.

The role of the FISC under the PAA was significantly reduced. It could only get involved if the recipient of an order for surveillance under the PAA challenged its legality.[484]

Under the PAA, surveillance could be authorised for periods up to a year by the Director of National Intelligence and the Attorney General for the 'acquisition of foreign intelligence information concerning persons reasonably

---

[479] Attorney General letter to Chairman Leahy and Senator Specter, January 17, 2007 <http://graphics8.nytimes.com/packages/pdf/politics/20060117gonzales_Letter.pdf> accessed 3 August 2014

[480] Protect America Act of 2007, Pub. L. No. 110-55, Aug 5 2007, 121 Stat. 552

[481] 50 USC S1805a (2006 and supp. 1 2008)

[482] Cardy (n 475) 185

[483] Cooper Blum (n 400) 296

[484] 50 USC S1805b(c) (2006 and supp. 1 2008)

believed to be outside the United States'.[485] In addition, there is no requirement to specify the 'specific facilities, places, premises, or property'[486] at which the surveillance is aimed, and a 'significant'[487] but not primary purpose must be to obtain foreign intelligence information.

Due to the fact that it was so controversial,[488] the PAA had a sunset clause to expire its provisions after only 6 months except that any authorisations already in effect would remain so.[489] Therefore, surveillance authorised the day before the sunset clause took effect could continue for up to a year regardless.

The PAA was challenged by Yahoo![490] which had been ordered to 'assist in warrantless surveillance of certain customers'[491] in 2007. The case went first to the FISC which ended with a threat of civil action against Yahoo! which then complied with the order at the same time requesting that the Foreign Intelligence Surveillance Court of Review (FISCR) examine the case.[492]

Yahoo! claimed that the government still needed a warrant and even if there were an exception to that rule, the surveillance was unreasonable and therefore violated the Fourth Amendment. The court found that there are cases not related to foreign intelligence which have '"special needs"'[493] when the requirement for a warrant would be excused, specifically when the

---

[485] 50 USC S1805b(a) (2006 and supp. 1 2008)

[486] 50 USC S1805b(b) (2006 and supp. 1 2008)

[487] 50 USC S1805b(a)(4) (2006 and supp. 1 2008)

[488] Cooper Blum (n 400) 297

[489] Protect America Act of 2007 (n 499) 557

[490] Yahoo! was not identified in the published court case 551 F.3d 1004, it's name being redacted throughout. However, Yahoo!'s name was revealed in FISC Docket No 105B(g) 07-01.

[491] In re Directives Pursuant to Section 105b of the Foreign Intelligence Surveillance Act, 551 F.3d 1004, 1007

[492] Ibid., 1008

[493] Ibid., 1009

'purpose behind the governmental action went well beyond routine law enforcement and insisting upon a warrant would materially interfere with the accomplishment of that purpose.'[494] Using the principles in these special needs cases, the court determined that surveillance under PAA 'possesses characteristics that qualify it'[495] for an exception to the warrant requirement. The court held that:

> a foreign intelligence exception to the Fourth Amendment's warrant requirement exists when surveillance is conducted to obtain foreign intelligence for national security purposes and is directed against foreign powers or agents of foreign powers reasonably believed to be located outside the United States.[496]

Despite this, the court did state that this does not give the government free reign. The Fourth Amendment protects from unreasonable searches and seizures and therefore, there is a reasonableness requirement. In assessing the reasonableness of the surveillance, the court considered the 'totality of the circumstances'[497] to balance the importance of the needs of the government against the Constitutional protections afforded to an individual. As the importance of the government's intrusion increases, so does the level of intrusion which may be tolerated under the Constitution.[498] The court determined that the government's need for the surveillance was high[499] and Yahoo! had not produced any evidence of harm, or potential major risk of error or abuse.[500] The court found the intrusions to satisfy the reasonableness test.[501]

---

[494] Ibid.

[495] Ibid., 1011

[496] Ibid., 1012

[497] Ibid.

[498] Ibid.

[499] Ibid.

[500] Ibid., 1013

[501] Ibid., 1016

FISA was once again modified by the FISA Amendments Act of 2008 (FAA).[502] The FAA replaced Title VII of FISA and repealed the PAA, thereby removing the redefinition of electronic surveillance which had allowed surveillance under the PAA to bypass the FISC.

FAA s.702 dealt with the surveilling of non-US persons located outside the US. Like the PAA, the FAA maintained the joint authorisation requirements of the Attorney General and Director of National Intelligence for surveillance of up to a year targeting people reasonably believed to be outside the US for the acquisition of foreign intelligence information.[503]

The FAA sets specific limitations such as it must not be used to intentionally target people in the US[504] or intentionally target someone outside the US with the intention of using that to target a specific known person in the US.[505] Furthermore, it must not be used to intentionally target US people outside of the US[506] nor intentionally acquire communications where all parties are located in the US.[507] The FAA also contains the condition that all acquisition of communications must be carried out in a manner consistent with the Fourth Amendment[508] and this must also be considered by the FISC.[509] However, as stated by Blum foreign nationals located overseas are not protected by the Fourth Amendment.[510]

---

[502] Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008, Pub. L. 110-261, 122 Stat. 2436, July 10, 2008

[503] FAA 702(a)

[504] FAA 702(b)(1)

[505] FAA 702(b)(2)

[506] FAA 702(b)(3)

[507] FAA 702(b)(4)

[508] FAA 702(b)(5)

[509] FAA 702(b)(i)(3)(A)

[510] Cooper Blum (n 400) 298-9

On the issue of retrospective immunity for communications providers, the FAA finally provided a solution. Like the PAA, the FAA essentially gave immunity to service providers going forward. However, in addition to this, it specifically provided immunity to any CSP which had provided assistance on surveillance that was authorised by the President between 11 September 2001 and 17 January 2007,[511] provided they had a written request from the Attorney General or intelligence community head or deputy stating the request was legal and authorised by the President.[512] As aforementioned, 17 January 2007 was the date on which the Attorney General informed the Senate that the TSP would not be re-authorised.

3.8.2 Bulk collection programs

As discussed above, three articles permit various collection of communications content and metadata, namely s.215 of the Patriot Act (Section 215), s.702 of the FAA (FAA 702), and EO12333. Actions under FAA 702 are examined in Chapter 6 along with the Snowden revelations.

On issuing a Section 215 order in 2013, the FISC noted that the provision of metadata is 'squarely controlled'[513] by *Smith v. Maryland*, the case which led to the Third Party Doctrine. Although the Court recognised that the Snowden revelations had resulted in 'unprecedented disclosures'[514] about Section 215 and other intelligence programs, it found nothing in the Constitution or law to prevent it issuing the order.

---

[511] FAA 802(a)(4)(A) 122 Stat. 2468-2469

[512] FAA 802(a)(4)(B) 122 Stat. 2469

[513] In Re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things, Docket Number BR 13-109, p6-9 <http://www.fisc.uscourts.gov/sites/default/files/BR%2013-109%20Order-1.pdf> accessed 3 July 2016

[514] Ibid., 29

Telephone records gathered under Section 215 were stored in a database by the NSA. Provided that there is 'reasonable, articulable suspicion'[515] that a number is associated with terrorism, analysts are able to chain up to 3 hops to look for associations, namely the first hop is all numbers in contact with the number being queried, the second hop is all numbers in contact with all those numbers revealed in the first hop and similarly, the third hop is all numbers in contact with all those numbers revealed in the second hop. If people have an average of 40 active contacts this could result in a chain containing over 2.5 million phone numbers.[516] The significant this surveillance has on privacy is clear.

The Privacy and Civil Liberties Oversight Board (PCLOB) determined that while Section 215 was designed to grant the FBI access to relevant business records, the NSAs telephone metadata program 'bears almost no resemblance'[517] of the original aim of Section 215. The potentially all-encompassing data collection could not be regarded as relevant to any FBI investigation as required by Section 215, and that requiring telephone companies to continually send metadata had no basis in Section 215 and was 'inconsistent with FISA as a whole.'[518] It was also determined that the program violated the ECPA which only permits telephone companies to share customer records with the government under certain circumstances and Section 215 is not among these.

The PCLOB was critical of the fact that such bulk metadata collection could reveal so much detail about a person's life that this could have a 'significant

---

[515] Ibid., 5

[516] 40*40*40*40 = 2,560,000; see <https://www.aclu.org/files/blog_images/DEM13-3Hops-JUMPS-V08.gif> accessed 20 December 2015

[517] Privacy and Civil Liberties Oversight Board, 'Report on the Telephone Records Program Conducted under Section 215 of the USA PATRIOT Act and on the Operations of the Foreign Intelligence Surveillance Court', January 23 2014, 10

[518] Ibid.

and detrimental effect on individual privacy.'[519] Furthermore, it was mindful of the potential for mission creep, the potential use of the information to target specific groups and the chilling effect that the program might have on the freedom of speech and association.[520] Moreover, it did not find any cases of threats to the US where telephone metadata had made any significant difference to investigations or directly aided the discovery of a terrorist plot.[521]

Bulk collection under Section 215 was finally halted by the USA FREEDOM Act of 2015.[522] Under the changes, the US Government would no longer be permitted to collect bulk telephony metadata after the 29 November 2015. Instead, specific telephone numbers would be sent to CSPs who would then produce the relevant records. This method was 'expected to be operationally sufficient'.[523] Although this is a positive outcome for communications privacy in the US, this research found that it has no bearing on bulk Internet metadata collection which is still carried out under different legislation as described above. Particularly, although the arguments are the same, it has no effect on the drag-net Internet surveillance revealed by Snowden and this is discussed in more detail in Chapter 6.

3.9 Conclusion

This chapter showed that the development of legislation in the US has followed changes in technology and changes in ways in which the intelligence and security agencies have carried out communications surveillance. From

---

[519] Ibid., 12

[520] Ibid.

[521] Ibid., 146

[522] Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline Over Monitoring Act of 2015, Pub. L. 114-23, June 2 2015, 129 Stat. 268

[523] Fact sheet: Implementation of the USA FREEDOM Act of 2015, November 27, 2015 <http://www.dni.gov/files/icotr/USAFA%20Implementation%20Fact%20Sheet.pdf> accessed 25 June 2016

the early days of *Olmstead*, the government has sought to carry out surveillance without judicial review and the courts have struggled to keep pace. *Katz* was a step change in surveillance with the courts extending Fourth Amendment protections and the formulation of a viable test of the expectation of privacy. The decision in *Keith* set the US on course to enact FISA. ECPA brought the law up to date regarding digital communications, and CALEA ensured that CSPs would maintain tapping ability in the Internet age.

The research reveals an ongoing cycle with legislation being modified to limit surveillance, followed by law enforcement or the executive encroaching on privacy once more, with the cycle beginning once again. Laws such as the PAA and FAA providing retrospective immunity for CSPs who were compelled to mount invasive surveillance show the ultimate desire to destroy Internet privacy. Some surveillance programs only became evident in 2013 as a result of the Snowden revelations. When one views the sheer amount of material that may be collected given the level of non-US Internet traffic that transits the US, these programs remain a major concern which becomes the subject to be discussed in Chapter 6. However, as the courts will react to legislative changes in order to maintain some protection of privacy one must hope that this will continue and that Internet privacy in the US, while in retreat is not yet dead. In the next chapter, Chapter 4, focus is now turned to Internet privacy and communications surveillance in the UK context.

This page is intentionally left blank

Chapter 4: Internet privacy and communications surveillance in UK

4.1 Introduction

Chapter 3 carried out an in-depth investigation of communications surveillance in the US context in order to explore whether or not Internet privacy still exists. It concluded that while the courts are willing to take steps to maintain privacy in the face of mass Internet surveillance programmes Internet privacy in the US still has a chance for survival. The aim of this chapter is to review the development of UK communications surveillance laws to examine how these may affect Internet privacy. The review includes those regional and supranational instruments that have a direct effect on the UK. Additionally, as with the previous chapter, the principal governmental interference with privacy considered here is communications surveillance because this encompasses Internet surveillance. Several key cases are examined and presented to illustrate as well as provide supportive evidence on the effect these cases had on the way UK surveillance law developed. As will be argued, like the US, surveillance laws in the UK have been shaped by several unfavourable court decisions.

4.2 Communications surveillance in the UK

As with the case of the US presented in Chapter 3, in order to understand Internet privacy and how the law may protect it, it is necessary first to examine the evolution of communications surveillance in the UK context. It is found that the authority to intercept communications in the UK has 'obscure'[524] origins. The first publically recorded requirement for a warrant for the interception of

---

[524] Privy Council, *Report of the Committee of Privy Councillors appointed to inquire into the interception of communications* (Cmnd 283, October 1957) p7 at (9) (Birkett Report)

communications in the UK dates back to 1663, but the practice of opening letters had been going on long before this.[525]

With the invention of the telegraph, the first interception laws were put into place making it an offence to intercept messages or disclose their content.[526] Changing technology meant that protection of telephone communications, which only became widespread in the 1880's, was not included.[527] This is evidently an early indication of the law's inability to cope with changes in technology which would become a theme where UK laws were concerned.

In fact, the Post Office held the view that the power to intercept communications exercised by the Crown was also held by 'any other operator of telephones'.[528] Because of this, warrants were not obtained, interception arrangements were being dealt with directly between the Post Office, the Security Service and/or the Police. This problem was addressed in 1937 and thereafter, it required a warrant from the Secretary of State.[529] Even so, it was not until 1969 that the defence of acting in accordance to a warrant was added by s.1(1) of Schedule 5 of the Post Office Act 1969.[530] Section 80 of that Act was drafted to ensure that interceptions by the Post Office would still be carried out on request from the Government. In spite of this, this was about to be tested in the ECtHR.

---

[525] Ibid.

[526] Telegraph Act 1868 s.20; see also Telegraph Act 1863 s.45; protection of Telegrams was added by the Post Office (Protection) Act 1884 s.11

[527] Alexander Graham Bell invented his telephone in 1875 and had the invention notarised in Boston on 20th January 1876. See Burns, R.W., Communications: an international history of the formative years (Institution of Electrical Engineers, London, 2004) p171

[528] Privy Council (n 524) p13 at (40)

[529] Ibid., p14 at (41)

[530] Post Office Act 1969, Schedule 5, 1(1); the Act created the Post Office as a public body.

4.2.1 Telephone interception – the Malone cases

As with the US, laws protecting Internet privacy and regulating surveillance in the UK can be traced back to the regulation of telephone interception. As found in this research, the Malone cases are significant as they would test the legality of telephone tapping in the UK in the high court and, later, the ECtHR.

Malone had been charged with handling stolen property and found not guilty. Realising his communications had been intercepted, Malone sought an injunction against the Police. Malone's claim in this case was that the interception had been unlawful, even if under a warrant signed by the Home Secretary, and that this breached his human rights under Arts 8 and 13 of the ECHR. In *Malone v Commissioner for the Metropolitan Police (no.2)*,[531] the Court determined that there had been no breach of the law regarding the telephone interception simply because 'there was no law against it',[532] and although not specifically permitted by law s.80 of the Post Office Act 1969 indicated that interception was lawful under warrant. There had been no trespass as the interception was carried out at an exchange.[533] On this point, it is worth noting that the ruling in *Malone* is similar to the 1928 ruling in *Olmstead*[534] in the US, over 50 years earlier (which was discussed in Chapter 3).

Malone had relied in part on *Klass v Germany*[535] in which the Court had noted that the 'mere existence'[536] of surveillance legislation can create a 'menace of surveillance'[537] which itself can potentially breach Art 8 of the ECHR by

---

[531] *Malone v Commissioner for the Metropolitan Police (no.2)* [1979] 344 Ch.

[532] Ibid., 345

[533] Ibid., 369

[534] Olmstead v. US, 277 US 438 (1928)

[535] *Klass and Others v Germany*, App. No. 5029/71, (ECtHR, 6 September 1978)

[536] Ibid., 41

[537] Ibid.

creating an environment where people are naturally concerned their communications may be surveilled. The Court did not find a breach of Art 8 because German laws were in place permitting surveillance and it was deemed necessary in a democratic society, thus passing the tests of Art 8(2). However, it was clear that the Court would set limits, there otherwise being the danger that democracy itself is destroyed by those trying to protect it.[538]

While the court in *Malone* noted that the law as it then stood would not withstand the scrutiny of the Strasbourg court it dismissed the case. The court did, however, highlight that the subject of telephone tapping 'cries out for legislation.'[539] The Government contested this, stating that if legislation were needed, it would set down appropriate safeguards and restrictions on interception.[540] After studying the *Malone* judgment, a Command Paper[541] (the 'White Paper') was released to bring up to date the account given in the Birkett report. Furthermore, the Home Secretary stated that, as interception needs to be done in secret it cannot be subjected to 'normal processes of parliamentary control.'[542] One may argue that the balance between State security and individual liberty should be the subject of legislation and be accountable to Parliament.[543] However, even after reminders that the UK is required to bring surveillance matters under statutory control as required by Art 8 of the ECHR,[544] in particular in the light of *Malone*,[545] no legislative changes were

---

[538] Ibid., 49

[539] *Malone v Commissioner for the Metropolitan Police (no.2)* [1979] 344 Ch. 346

[540] HC Deb 08 March 1979 vol 963 at 751

[541] Home Office, *The Interception of Communications in Great Britain* (Cmnd. 7873, 1980)

[542] HC Deb 01 April 1980 vol 982 cc205-220 at 207

[543] Ibid., 214

[544] The Royal Commission on Criminal Procedure, (Cmnd 8092, January 1981), 3.56

[545] Ibid., 3.60

proposed. This inaction on the part of the government would offer little protection from the scrutiny of the Strasbourg court as *Malone* took his case there.

4.2.2 The Telecommunications Act

The Conservative government elected in 1983 was committed to privatising telecommunication services, which it progressed via the Telecommunications Act 1984 which removed BTs exclusivity with regard to the provision of such services. However, privatisation would lead to private organisations potentially carrying out telephone intercepts with no effective legal control.[546] As *Malone* had brought surveillance into the public eye there was concern that surveillance not covered by statute would always be viewed with suspicion.[547]

The Telecommunications Act 1984 did make it an offence to intentionally intercept a message[548] as well as intentionally disclosing the contents of any intercepted message.[549] However, no offence is committed if the interception is carried out under a warrant from the Secretary of State, and it is not an offence to disclose the contents of intercepts if it is done in connection with the investigation of *any* criminal offence.[550] The Act gave the Secretary of State the ability to direct public telecommunications operators 'to do, or not to do, a particular thing'[551] in the interests of national security. Also, the operator could be prevented from revealing the fact that any actions had taken place. In fact, this research found that this lose, nondescript language would later be

---

[546] Ian J Lloyd, 'The Interception of Communications Act 1985', 49 MLR January 1986 86-95 at 88

[547] HL Deb 19 March 1984 vol 449 cc977-1036 at 1032

[548] Telecommunications Act 1984 s.45(1)(a)

[549] Ibid., s.45(1)(b)

[550] Ibid., s.45(3)

[551] Ibid., s.94

relied upon by the UK government to permit bulk metadata collection which will be discussed in Section 4.5 below.

4.2.3 The Interception of Communications Act

Having exhausted national remedies, Malone took his case to the ECHR. There was no question that the interception of communications performed under a warrant issued by the Secretary of State was lawful under UK law.[552] However, the major issue was determining whether or not the law had any control over how and why warrants were issued in order to comply with Art 8(2).[553]

The analysis of the Commission focussed on s.80 of the Post Office Act 1969 which the government claimed provided a statutory basis for the issuing of interception warrants by copying into law previous practices. However, no legal restriction as to what a minister could impose on the Postmaster General prior to the Act could be found.[554] Furthermore, the issuing of a warrant by the Secretary of State was an administrative practice not defined in law.[555] Because of this, the Commission found it uncertain that the law laid down any conditions or procedures for the issuing of interception warrants. It therefore concluded that this was a breach of Art 8(2)[556] and thus, a breach of Malone's Art 8 rights.[557] The Court concurred.

The Act passed to address the issues highlighted in *Malone* was the Interception of Communications Act 1985 (IOCA). It made it an offence to intercept communications being transmitted by post or public

---

[552] European Commission on Human Rights, App No 8691/79 James Malone against United Kingdom, 17 December 1981, at 125

[553] Ibid., at 126

[554] Ibid., at 138

[555] Ibid., at 139

[556] Ibid., at 144

[557] Ibid., at 145

telecommunication systems unless a warrant had been issued by the Secretary of State.[558] Warrants could be issued on grounds of national security[559] to prevent or detect serious crime,[560] or to safeguard the economic wellbeing of the UK.[561] IOCA thus finally put authority for interception on a statutory basis.

ECHR jurisprudence resulted in further changes in UK law. In *Hewitt and Harman v United Kingdom*[562] the court found that surveillance was not in accordance with law because the relevant law was not in statute. It found that the surveillance of Hewitt and Harman had breached their Art 8 rights. This was rectified by the enactment of the Security Services Act 1989 which put the service on a statutory basis, stating there would 'continue to be'[563] such a service.

IOCA was found to provide the necessary statutory basis in the case of *Christie v United Kingdom*[564]. In this case, the applicant alleged that GCHQ had intercepted trades union telexes addressed to him. The government neither confirmed nor denied this, but accepted that it might have happened. The Commission determined that, as procedures for interception were set out in IOCA and the Security Services Act 1989, the interference was in accordance with law. Furthermore, the law was accessible as it was set out in statute. The case was declared as inadmissible.

---

[558] Interception of Communications Act 1985 (IOCA) s.1

[559] Ibid., s.2(2)(a)

[560] Ibid., s.2(2)(b)

[561] Ibid., s.2(2)(c)

[562] *Hewitt and Harman v United Kingdom*, App No 12175/86 (Commission, 9 May 1989)

[563] Security Service Act 1989, s.1(1)

[564] *Christie v United Kingdom*, App No 21482/93 (Commission, 27 June 1994)

However, IOCA was only designed to provide a statutory basis for the interception of communications carried by public systems. The Government reasoned that as communications would at some point traverse the public system, it did not need to legislate for private systems connected to it. By not considering fully the technologies available at the time, the Government had ignored the issue of the point of interception, which itself may lie outside of the public system and would therefore be unprotected by IOCA. This was evidently shown in the case in *R v Effick and Mitchell*[565] in which the House of Lords held that a cordless telephone was not a part of the public telecommunications system. In this case, when a cordless telephone was used, the police could pick up the conversations by the use of a radio receiver. No warrant had been obtained for the surveillance[566] and yet, because IOCA did not cover private systems, the interception was not prohibited.[567] Unfortunately, this case was not taken to the ECHR. However, the lack of coverage of private networks would be tested by the ECHR in *Halford v United Kingdom*[568] which is presented next.

4.2.4 Halford: the issue of private communications systems

The next important case in the evolution of interception legislation in the UK was *Halford v United Kingdom*. Halford was an Assistant Chief Constable. She had applied for promotion, but the Chief Constable had recommended against this, allegedly because he objected to her views on equality between men and women.[569] She commenced proceedings in an industrial tribunal.

---

[565] *R v Effick and Mitchell* (1994) 99 Cr App Rep 312

[566] Ibid., 314

[567] Ibid., 315

[568] *Halford v The United Kingdom*, App. No. 20605/92, (ECtHR, 25 June 1997)

[569] Ibid., 10

She had an office with two telephones, one of which was provided for private use.[570] These telephones were connected to the internal police telephone network which was a private system, not a part of the public telecommunications system. She had been assured by the Chief Constable that she could use her office phone in relation to the ongoing tribunal case. She alleged that both her home and office telephone communications had been subjected to interception to obtain information to use against her in the tribunal,[571] and provided evidence of this.[572] The Government accepted she had established a 'reasonable likelihood'[573] that her office telephone communications had been intercepted.

Halford raised her concerns about this interception at a tribunal hearing. However, IOCA s.9 excludes the use of intercept evidence in court or tribunals.[574] On submission to the Interception of Communications Tribunal, she was informed that there had been no breach of IOCA s.2-5,[575] which the Court took to mean that either an offence had been committed under IOCA s.1 or that an intercept warrant had been issued.[576]

Although the Government argued that employers should be able to monitor calls made by employees on telephones provided by the employer,[577] the Court determined that Halford had a 'reasonable expectation of privacy',[578] in

---

[570] Ibid., 16

[571] Ibid., 17

[572] See European Commission on Human Rights, Plenary Commission, App. No. 20605/92, Alison Halford against the United Kingdom, 18 April 1996, at 21 for a list of this evidence

[573] Halford (n 568) 17

[574] Ibid., 18

[575] Ibid., 19

[576] Ibid., 25

[577] Ibid., 43

[578] Ibid., 45

particular as she had a private office and a telephone for private use. However, the fact that IOCA was not written to cover private telecommunications systems was critical. This is because there was effectively no law covering the interception meaning that Halford's Art 8 rights had been breached because the action was not in accordance with the law.[579] Enacted because of the ruling in *Malone*, IOCA's failing in *Halford* would lead to new legislation being introduced. That new legislation was the Regulation of Investigatory Powers Act 2000 (RIPA) but it was not enacted in time to prevent adverse rulings in two more cases - Copland and Liberty - heard by the Strasbourg court, both of which were actually decided some years after RIPA was in place. These two cases are discussed next.

4.2.5 Copland: the issue of workplace surveillance

The ruling in the *Halford* case provided a recognition of privacy in the work place with regard to private telephone communications.[580] In the case of *Copland v United Kingdom*,[581] the ECtHR extended this to cover the monitoring of an employee's e-mails and Internet usage.[582]

Copland had had her phone, e-mail and Internet usage monitored by her employer, Carmarthenshire College. This included analysis of the telephone bills but more significantly, included an analysis of the websites she visited along with an investigation into her e-mails[583]. The Court found that Copland had a 'reasonable expectation of privacy'[584] because she had not been warned that her communications might be monitored. It had further issue with

---

[579] Ibid., 51

[580] Lothar Determann and Robert Sprague, 'Intrusive monitoring: employee privacy, expectations are reasonable in Europe, destroyed in the United States', 26 Berkeley Tech. L.J. 979 2011 p1020

[581] *Copland v United Kingdom*, App No 62617/00 (ECtHR, 3 April 2007)

[582] Ibid., 41

[583] Ibid., 10 - 12

[584] Ibid., 42

the fact that data about Copland's telephone and Internet usage were recorded and stored.[585] The Court found that Art 8 had been breached as there was no UK law regulating monitoring of employee communications at the time.[586] This research has, once again, found another supportive evidence to indicate the law's inability to cope with or keep pace with changes and/or advances in technology.

The *Copland* case was submitted to the ECHR at a time when the UK was about to introduce RIPA to regulate surveillance.[587] It did, however, indicate that Art 8 of the ECHR had expanded to include workplace communications and could and would encompass Internet communications.

4.2.6 Liberty: pre-Snowden mass surveillance

The case of *Liberty and Others v United Kingdom*[588] shows just how far the Government was prepared to go to intercept communications in the 1990s. This case surrounds the construction of a tower at Capenhurst in Cheshire which was allegedly positioned in such a way as to be able to intercept the microwave beam linking to British Telecom radio stations in Clwyd and Chester. Telecommunications passing across this link would include much of that going to and from Ireland.[589]

The legality of mass surveillance had been tested in the Strasbourg court previously in *Weber and Saravia v Germany*[590] which built on *Klass*. In *Weber* the applicants claimed that by carrying out mass surveillance to determine if

---

[585] Ibid., 43-44

[586] Ibid., 48

[587] Copland was decided in 2007 but the case was submitted to the Court on 23 May 2000. Although Copland mentioned the Regulation of Investigatory Powers Act that Act was not in force at the time.

[588] *Liberty and Others v United Kingdom*, App. No. 58243/00, (ECtHR, 1 July, 2008)

[589] Ibid., 5

[590] *Weber and Saravia v Germany*, app. no. 54934/00, 29 June 2006

there was the danger of an armed attack Germany had breached their Art. 8 rights. The Court found that the methods and reasons by which communications were selected out of all of those intercepted were defined in legislation as were the procedures for sharing, retaining or destroying such communications. It concluded that there were sufficient safeguards against arbitrary interference with Art. 8 rights and found that the interference was in accordance with law.[591] The Court further determined that the actions of the German government in mounting mass surveillance coupled with the safeguards present in German law were such that Germany was entitled to consider the privacy invasions to be necessary in a democratic society for the protection of its national security and fight against crime.[592] The application was declared inadmissible.[593]

Applying this *Weber* test to *Liberty* the Court found that the government was not acting in accordance with the law.[594] The Court argued that warrants under IOCA s.3(2) could be extremely broad in scope with 'no limit to the type of external communications'[595] that could be included. The government confirmed that 'in principle',[596] anyone sending or receiving telecommunications outside the UK could have had those intercepted under an IOCA s.3(2) warrant. IOCA was further criticised by the Court because the methods to be employed to determine which communications, out of all the intercepted communications were to be examined, were not publically available.[597] The Court found there had been a breach of Art 8.

---

[591] Ibid., 102

[592] Ibid., 137

[593] Liberty (n 588) 96-100

[594] Ibid. 45

[595] Ibid., 64

[596] Ibid., 64

[597] Ibid., 66

In *Weber* the Court had by now developed a three part test for when determining if an interference was in accordance with the law. First, there must be a basis in domestic law; second, the domestic law must be compatible with the rule of law and must be accessible to the citizen concerned; and third, the affected citizen must be able to foresee the effect that law may have upon them. Expanding on the foreseeability of the effect of law in the special case of national security the Court added that in such cases, there is not a requirement that an individual can foresee when they are likely to be targeted and thus adapt to avoid surveillance. However, there must be clearly defined rules on interception to ensure that any interference with privacy is not arbitrary. The Court noted that this is particularly important given the rate of change of technology.[598]

The use of technology which led to this case bears a stark resemblance to methods allegedly used to tap into Internet connections revealed in the Snowden revelations in 2013 as discussed and presented in Chapter 6.

4.3 The Regulation of Investigatory Powers Act, 2000 (RIPA)

Since the enactment of IOCA, the telecommunications sector had expanded, in particular with mobile phones and Internet use becoming more widespread. It was noted in a government consultation paper that IOCA had not kept up and yet, 'criminals and terrorists had been quick to exploit'[599] these new services. The paper also noted the adverse decision in *Halford*, mentioning that private networks must be covered.

In order to regulate surveillance and ensure it was brought into line with ECHR jurisprudence, the Government enacted RIPA which was described during its passage as a 'significant step forward for the protection of human rights'.[600] Indeed, on the face of it, RIPA was legislation aimed at legitimising

---

[598] Weber (n 590) 93

[599] Home Office, *Interception of Communications in the United Kingdom: a consultation paper* (Cm. 4368, June 1999), 3

[600] HC Deb 06 March 2000 vol 345 cc767-835 at 767

interception of communications while at the same time protecting human rights. However, critics described it as 'hastily drafted and ill-conceived legislation that is merely reactive and not proactive',[601] as it was not so much protecting human rights as protecting the large number of authorities 'from the consequences of actions that would otherwise be unlawful'[602] under the HRA.

RIPA addressed a major flaw in IOCA by making it not only an offence to unlawfully intercept communications carried by public postal[603] or telecommunications systems,[604] but also those carried by private telecommunications systems.[605] The research found that not only was this important in addressing the failings of IOCA, but it was also particularly significant from the Government's perspective if RIPA were to have any effect on the Internet which is operated predominantly by private companies. This is because even where Internet traffic passes across a public network and could thus be intercepted under IOCA, it is more efficient to intercept at the ISP concerned.[606] Furthermore, RIPA also allowed interception of all communication of a target person and was not bound to a particular telephone or address. Additionally, it dealt with the transmission of communications 'by any means',[607] of great importance when considering the many and varied methods of Internet communications.

The government also wanted to be able to use interception earlier than was possible under IOCA. Section 2(3) of IOCA required the Secretary of State to consider if the information sought could be obtained in other ways before

---

[601] Alan S Reid and Nicholas Ryder, 'For whose eyes only? A critique of the United Kingdom's Regulation of Investigatory Powers Act 2000', Information & Communications Technology Law, 10:2, 179-201 at 179

[602] Cousens (n 138) 3

[603] Regulation of Investigatory Powers Act 2000 (RIPA) s.1(1)(a)

[604] Ibid., s.1(1)(b)

[605] Ibid., s.1(2)

[606] Home Office (n 599), 3.7

[607] RIPA (n 603) s.2(1)

signing a warrant for interception.[608] The government was concerned that this meant interception was only used in the most serious cases and as a last resort.[609]

RIPA also required CSPs to 'take reasonable steps to ensure that their system is capable of being intercepted.'[610] Although an intercept warrant under IOCA would require a CSP to comply, no account was made of that CSPs ability to comply. While recognising that smaller CSPs may have difficulty in complying technically with a warrant, it decided to force them all to comply anyway. The costs to a CSP of providing intercept capabilities would be contributed to from government funds.[611] As previously discussed in Chapter 3, this requirement compares to that set out by CALEA in the US.

RIPA intercept warrants are issued by a Secretary of State who is required to ensure that the warrant is proportionate[612] and necessary for national security purposes,[613] or for the detection or prevention of serious crime,[614] or for safeguarding the economic wellbeing of the UK.[615] However, in addition to this, a warrant can be issued for the purposes of assisting, under mutual assistance agreements other jurisdictions in the detection or prevention of serious crime.[616] These warrants are quite broad. They permit, for example the interception of communications not identified in the warrant where this is

---

[608] IOCA (n 558) s.2(3)

[609] Home Office (n599), 3.2

[610] Ibid., 5.3; RIPA (n 603) s.12

[611] Ibid., s.14

[612] Ibid., s.5(2)(b)

[613] Ibid., s.5(3)(a)

[614] Ibid., s.5(3)(b)

[615] Ibid., s.5(3)(c)

[616] Ibid., s.5(3)(d)

necessary in order to carry out the intended authorised interception.[617] The warrants also provide authorisation to obtain all associated metadata.[618] As Taylor points out it is possible to use this data to construct a 'very comprehensive dossier on an individual's private life',[619] potentially to a far greater extent that access to the content of communications may provide.[620]

A RIPA warrant must specify either a single person[621] or a single set of premises[622] as the subject of the interception. However, these restrictions are not applicable where the warrant is for the interception of 'external communications'[623] in transit in a telecommunication system. This permitted GCHQ to run a programme named Tempora, revealed in the Snowden revelations, which involved tapping subsea cables to copy off Internet traffic. The implications of this all-encompassing interception provision will be discussed further and presented in Chapter 6.

4.3.1 Kennedy v The United Kingdom

Although RIPA is complex legislation the government published a code of practice detailing its operation and made this available via the Web on 1 July 2002.[624] This aided the government in the ruling by the ECtHR in *Kennedy v*

---

[617] Ibid., s.5(6)(a)

[618] Ibid., s.5(6)(b)

[619] Nick W Taylor, 'Policing, privacy and proportionality', EHRLR 2003, Supp (special issue: privacy 2003) at 97

[620] Justice, Protecting the Public in a Changing Communications Environment: JUSTICE Response to the Home Office Consultation, July 2009, at 2

[621] Ibid., s.8(1)(a)

[622] Ibid., s.8(1)(b)

[623] Ibid., s.8(5)(a)

[624] Home Office, *Interception of Communications Code of Practice Pursuant to section 71 of the Regulation of Investigatory Powers Act 2000*

The United Kingdom.[625] Kennedy had been convicted of murder but released on appeal. He believed that his communications were being intercepted and that this had an effect on his business. He further believed the intelligence agencies were continually renewing an intercept warrant targeting his communications in order to disrupt his business.[626]

Having attempted a Subject Access Request under the DPA which was denied on the grounds of national security he complained to the Investigatory Powers Tribunal (IPT) which did not find in his favour. The ECtHR noted that this either means there had been no interception or that there had and it was lawful.[627] On the issue of renewed warrants the Court was satisfied that the rules in RIPA regarding the renewal of warrants would have been followed and are also subject to the scrutiny of the Interception of Communications Commissioner. Finding that RIPA, in conjunction with the Code of Practice is sufficiently clear and there being no evidence of shortcomings the Court found that there had been no violation of Art.8.[628]

Kennedy served both to endorse RIPA as being ECHR-compliant and also to confirm that the ECtHR regarded the IPT as an 'independent and impartial body'[629] not constrained by the government or security services. The independence of any oversight body is an important factor when the ECtHR judges potential abuses.[630]

When one considers RIPA's US counterpart, FISA differs significantly in the terms of privacy protection. FISA treats US people differently from the rest of

---

[625] Kennedy v The United Kingdom, App. No. 26839/05 (ECtHR 18 May 2010)

[626] Ibid., 7

[627] Ibid., 20

[628] Ibid., 169-170

[629] Ibid., 167

[630] Sarah Eskens, Ot van Daalen and Nico van Eijk, '10 Standards or Oversight and Transparency of National Intelligence Services', 8 J. Nat'l Sec. L. & Pol'y 553 2015-2016, 576

the world and is more protective of them, whereas RIPA, in particular when one considers s.8(4) is extremely broad and all-encompassing. RIPA also contained provisions to grant access to communications data.[631] This is discussed next.

4.4 Increased surveillance after 9/11

As with the US, 9/11 caused a step-change in the intensification of Internet surveillance and the associated invasion of privacy. One day after the events of 9/11, legislation in the form of the Anti-terrorism, Crime and Security Act 2001 (ATCSA) was presented to Parliament. Part 11 of the Act deals with the retention of metadata. Section 102 of the Act stated that the Secretary of State would introduce a code of practice relating to data retention, after a strict process where the code is published[632] and passed by Parliament[633] after consultation with both the Information Commissioner[634] and with CSPs that would be affected by it.[635] Section 104 gave the Home Secretary the power to require CSPs to retain metadata for periods which would be specified in secondary legislation. However, this research found that the UK was not alone in the desire to retain metadata.

In its conclusions of 20 September 2001, the Justice and Home Affairs Council of the EU requested that the European Commission proposed ways to ensure that law enforcement agencies could 'investigate criminal acts involving the use of electronic communications systems'.[636] The Council indicated that it would find a balance between the need to protect personal information and

---

631 RIPA (n 603) Part 1 Chapter 2

632 Anti-terrorism, Crime and Security Act 2001 (ATCSA) s.103(1)

633 Ibid., s.103(4)

634 Ibid., s.103(2)(a)

635 Ibid., s.103(2)(b)

636 Conclusions adopted by the Council (Justice and Home Affairs), Brussels, 20 September 2001, SN 3926/6/01, at 4

the needs of law enforcement to access such information.[637] Although this was a high level statement not relating to any particular techniques, the Council's statement raised concerns with the European Data Protection Commissioners who released a statement via the Article 29 Working Party that data retention would be an 'improper invasion of the fundamental rights'[638] that people enjoy under Art. 8 of the ECHR, with retention for any period longer than the limited time permitted under Art 15(1) of the Directive on Privacy and Electronic Communications[639] being 'disproportionate and therefore unacceptable'.[640]

Although the Council's 2001 statement did not explicitly mention metadata, this was addressed in 2002. In its conclusions of 19 December 2002, the Council urged that all parties engage in dialogue both at national and EU level to find solutions to the 'issue of traffic data retention'[641] to enable it to be used for the 'prevention, detection, investigation and prosecution of criminal offences'[642] while protecting the fundamental rights and freedoms of citizens. Of note, this statement was dealing specifically with organised crime, not terrorism.

4.4.1 The UK voluntary code of practice

In the UK, the data retention powers under ATCSA were never brought into force. The Act included a sunset clause which would cause the code of

---

[637] Ibid.

[638] Article 29 Data Protection Working Party, Opinion 5/2002 on the Statement of the European Data Protection Commissioners at the International Conference in Cardiff (9-11 September 2002) on mandatory systematic retention of telecommunication traffic data, 11818/02/EN/Final, WP 64, 11 October 2002

[639] Directive 2002/58/EC (n 273)

[640] Article 29 Data Protection Working Party (n 638)

[641] Council conclusions of 19 December 2002 on information technology and the investigation and prosecution or organised crime, at 6

[642] Ibid.

practice to expire unless renewed. This was set initially for two years from the passing of the Act.[643] It was extended twice, in 2003[644] and 2005,[645] but after this, it allowed it to lapse.[646] By this time, European legislation was being discussed. Instead, it introduced a voluntary code of practice in 2003,[647] under which retained data must be made available on request from relevant authorities as set out in Chapter II Part I of RIPA meaning it would be available to 'any public authority'.[648] The Joint Committee on Human Rights questioned the legitimacy of the data retention regime, given that data would be available to agencies other than those tasked with national security.[649] As stated by Walker and Akdeniz, while the retention of data for national security purposes may be acceptable, it 'does not necessarily mean that blanket retention is justified'.[650]

4.4.2 The effects of the Madrid and London bombings

Terrorist attacks resulted in renewed attempts to create laws regarding metadata retention. In its Declaration on Combating Terrorism in the wake of the terrorist attack in Madrid of 11 March 2004, the European Council stated

---

[643] ATCSA (n 632) s.105

[644] The Retention of Communications Data (Extension of Initial Period) Order 2003, SI 2003/3173 extended the term for two years

[645] The Retention of Communications Data (Further Extension of Initial Period) Order 2005, SI 2005/3335 extended the term for a further two years

[646] Ian Brown, Regulation of converged communications surveillance, SSRN id 1261192, 2009

[647] The Retention of Communications Data (Code of Practice) Order 2003, SI 2003/3175

[648] RIPA (n 603) s.25(1)(g)

[649] Joint Committee on Human Rights 'Draft Voluntary Code of Practice on Retention of Communications Data under Part 11 of the Anti-terrorism, Crime and Security Act 2001' HL Paper 181, HC 1272 (2002-03) at 7c

[650] Clive Walker and Yaman Akdeniz, 'Anti-Terrorism Laws and Data Retention: War is Over?', 54 Northern Ireland Legal Quarterly 2, 159-182 at 174

that it would examine proposals for the establishment of rules on the retention of metadata by providers, with a view to these being adopted by June 2005.[651]

A proposal by France, Ireland, Sweden and the UK on 28 April 2004 stressed the need to retain metadata,[652] making it clear that identifying which data was required may not be possible perhaps for years after the communication was made.[653] The proposal also relied on the permission to retain data as set out in Art 15 of the Directive on Privacy and Electronic Communications.[654] While the proposal specified the retention of data 'for the purposes of the prevention, investigation, detection and prosecution of crime and criminal offences'[655] it included terrorism in the definition of criminal offences.[656] The proposal was initially rejected by the European Parliament, but the London bombings of 7 July 2005 put them back on the European Council's agenda, the presidency of which had just passed to the UK.[657] It was followed shortly after by the

---

[651] European Council, Declaration on Combating Terrorism, Brussels, 25 March 2004

[652] Council of the European Union, Draft Framework Decision on the retention of data processed and stored in connection with the provision of publicly available electronic communications services or data on public communications networks for the purpose of prevention, investigation, detection and prosecution of crime and criminal offences including terrorism, Brussels, 28 April 2004, 8958/04, at 5

[653] Ibid., at 6

[654] Directive 2002/58/EC (n 273)

[655] Council of the European Union, Draft Framework Decision (n 652) at 7

[656] The addendum to the proposal pointed out that it was a coincidence that it had been developed when terrorism was in the news and, consequently it was directed at both criminal and terrorist acts; see Council of the European Union, Explanatory Memorandum Framework Decision on the Retention of Communications Data (doc. 8958/04), Brussels, 20 December 2004, 8958/04 ADD 1, page 3

[657] Claire Walker, 'Data retention in the UK: pragmatic and proportionate, or a step too far?', Computer Law & Security Review, V25, issue 4, July 2009, pp325-2334 at 6.1 at 1.3

European Commission's own proposal,[658] which itself was followed by a highly critical Opinion from the Art 29 WP,[659] which stated that data retention would interfere with the 'inviolable, fundamental right to confidential communications.'[660] This would become the Data Retention Directive and is covered next.

4.4.3 The Data Retention Directive

The Data Retention Directive[661] (DRD) was adopted on 15 March 2006. The Directive set out the types of data which must be retained. Regarding the Internet, the data to be retained includes the connection date and time, userid and IP address,[662] and the calling telephone number[663] or digital subscriber line[664] of the source of the communication. For VoIP calls, the userids used, the telephone number and name and address for both subscriber[665] and

---

[658] Commission of the European Communities, 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) 438 final, Brussels, 21 September 2005

[659] Article 29 Data Protection Working Party, Opinion 4/2005 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)438 final of 21.09.2005), WP 113

[660] Ibid., executive summary

[661] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks amending Directive 2002/58/EC

[662] Ibid., Art. 5(1)(c)(2)(i)

[663] Ibid., Art. 5(1)(e)(3)(i)

[664] Ibid., Art. 5(1)(e)(3)(ii)

[665] Ibid., Art. 5(1)(a)(2)

recipient[666] must be retained. For mobile calls, cell location at the start[667], and all cell locations during the communication[668] must be retained. It can thus be seen that each Internet user will leave at the very least data showing their IP address and the date and time they connected while mobile users would leave a great deal more. The Directive was incorporated into UK law in two stages. The Data Retention (EC Directive) Regulations 2007 entered force on 1 October 2007 and implemented retention of communications data from telephony. This was superseded by the Data Retention (EC Directive) Regulations 2009 which included Internet data, entering into force on 6 April 2009.

It is found by this research that data retention as defined by the Directive has some fundamental flaws. Its aim to harmonise the provisions across the community falls short because of the flexibility in retention times. For example, where law enforcement is interested in who communicated with a given person after 12 months, data relating to calls from a State with a retention period of less than 12 months would have been deleted. The communications methods are also too specific, covering fixed and mobile and Voice over IP (VoIP) but no other forms of synchronous communication such as Instant Messengers.[669] It is somewhat surprising that this popular communications mechanism was overlooked. In fact, as echoed by Walker, the research found that even as the Data Retention (EC Directive) Regulations 2009 were implemented, the Government were already aware that they were inadequate.[670] In a consultation launched in 2009, the Government stressed that changes in the communications industry could undermine the effectiveness of metadata gathered under the current legislation. In sum, this

---

[666] Ibid., Art. 5(1)(b)(2)

[667] Ibid., Art. 5(1)(f)(1)

[668] Ibid., Art. 5(1)(f)(2)

[669] Instant Messenger services such as Internet Relay Chat (IRC) are among the older services on the Internet; IRC dates from 1988 and before that bulletin boards could be used for asynchronous exchanges

[670] Claire Walker (n 657) 6.1

research evidently demonstrated that the Government wanted access to a lot more and as a result the Intercept Modernisation Programme (IMP) was launched.

4.4.4 Interception Modernisation Programme

In 2008, the then Labour Government announced plans to create a centralised database to store all communications metadata for a 12-month period. Sensationalised in the Press as 'Orwellian',[671] the Information Commissioner described this as 'a step too far for the British way of life'.[672] The proposal was later dropped. The Government next attempted a public consultation on the issue in which three options were put forward, namely to do nothing, amass a huge central database of metadata which was rejected,[673] or require CSPs to retain, in addition to data already retained, data relating to third-party traffic passing across their networks which does not come under the Data Retention Directive.[674] The third option was the proposal that was put forward.

The Government proposed not only to require CSPs to retain third-party data, but also to process this third-party data, linking it where possible to their own data. This may be feasible, for example, where the various data comes from the same person or device.[675] This would represent a step change, seeing CSPs creating and then storing new data by combining their own data with that provided by others.[676] CSPs would need a mechanism to determine what of the data passing through their networks was, in fact, metadata. To do this,

---

[671] See http://news.bbc.co.uk/1/hi/uk_politics/7671046.stm accessed 7/4/15

[672] See http://www.theguardian.com/uk/2008/jul/15/privacy.internet accessed 7/4/15

[673] Home Office, *Protecting the Public in a Changing Communications Environment* (Cm 7586, 2009) 25

[674] Ibid., 26

[675] Ibid., 27

[676] The Information Commissioner's response to "Protecting the Public in a Changing Communications Environment", 15 July 2009, 1.6

CSPs would need to read and then analyse all data using a technique called Deep Packet Inspection (DPI).[677] The LSE points out that DPI constitutes an interception under RIPA s.1 and thus, is illegal without a warrant.[678] Therefore, the Government would need to introduce new legislation to cater for this. However, the Labour Government shelved the programme and left power after the 2010 general elections.

Clearly, the incoming Coalition Government were not about to abandon their desire for more metadata. While the Coalition gave some hope by stating they would 'end the storage of internet and email records without good reason',[679] this statement gave no illusion that the Government could not find a 'good reason' to continue to store such data. The finding was backed up by an action in the draft structural reform plan relating to the protection of people's freedoms which included the requirement to publish proposals for the 'storage of internet and e-mail records, including introducing legislation if necessary'.[680] IMP was revived under the name Communications Capabilities Development Programme (CCDP). Proposed legislation surfaced in the form of the Draft Communications Data Bill in June 2012. It maintained the IMP's concept of processing of third-party data in the form of filtering.

Processing third-party data, no matter in what name is extremely invasive as found in this research. Assembling data from all sources would potentially create a profile of every user. This has major privacy implications such as a

---

[677] Deep Packet Inspection (DPI) refers to the process of examining the data within a data packet rather than just the header information required to route the packet to its destination. It will thus gain access to all data within the packet, regardless of if it is metadata or content. DPI is covered in Chapter 6.

[678] LSE, Briefing on the Interception Modernisation Programme, PEN paper 5, p21

[679] The Coalition: our programme for government, May 2010, p11

[680] Home Office, *Draft Structural Reform Plan*, July 2010, p9

dramatic shift of the balance away from privacy in favour of the State's ability to know what everyone is doing online.[681]

The Bill made no attempt to analyse the changes which would be required to technology. Networks are built in a way which allows traffic to bypass failures or bottlenecks caused by overloading. If networks are redesigned to ensure that all data, including third party data can be captured and analysed, then this resilience is negated. Evidently, this research illustrates that having all data pass a single point creates a single point of failure and a possible bottleneck.[682] Furthermore, having the knowledge that all traffic is being analysed in the way proposed may well speed up the adoption of encryption as the norm rather than the choice. This could put third party traffic beyond the reach of retention plans.[683]

4.4.5 Challenges to Data retention & bulk interception

The implementation of the Data Retention Directive was not smooth. On 6 July 2006, Ireland, with the support of Slovakia, brought an action in the CJEU requesting the annulment of the Directive.[684] Their grounds were that the adoption of the Directive was not on an appropriate legal basis. Ireland argued that the Directive had been based on Art. 95 EC and therefore, must be aimed at improving the internal market by the harmonisation of national laws. Ireland contended that the Directive's aim was law enforcement and should have been based on Title VI of the EU Treaty. However, the Council and the Commission argued that the disparity of retention schemes across the community meant that the Directive was protecting and unifying the internal market. Therefore, the basis was correct. The Court dismissed the action. However, the Court noted that it was dealing solely with the legal basis and

---

681 House of Lords, House of Commons, *Joint Committee on Draft Communications Data Bill, session 2012-13, written evidence* p371

682 Ibid., p281 and 293

683 Ibid., p281

684 Case C-301/06, *Ireland v Parliament and Council* (Grand Chamber, 10 February 2009)

not ‘any possible infringement of fundamental rights’[685] caused by actions taken under the DRD.

There were other legal challenges in a number of EU States which resulted in delays or redrafting of national laws.[686] However, in 2010, not only did Germany find the transposed laws to be unconstitutional but it also annulled the Directive. As a result, the European Commission commenced legal action against Germany in 2012.[687] However, action brought before the High Court of Ireland by Digital Rights Ltd on 11 August 2006 resulted in that Court referring the question of validity of the DRD to the CJEU.[688] This action was joined by a request from the Austrian Verfassungsgerichtshof. Additionally, a request for judicial review of the 2009 Data Retention Directive was brought in 2011 by Tracey Cosgrove,[689] but was stayed pending the outcome of CJEU judgment. That judgment came on 8 April, 2014 in the joined cases C-293/12 and C-594/12.

The Court noted that metadata can provide very accurate information about people, their habits, where they live, where they go and who they meet.[690] It further noted that that the retention and use of data without even informing the

---

[685] Ibid., 57

[686] See generally Chris Jones and Ben Hayes, The EU Data Retention Directive: a case study in the legitimacy and effectiveness of EU counter-terrorism policy <http://secile.eu/wp-content/uploads/2013/11/Data-Retention-Directive-in-Europe-A-Case-Study.pdf> accessed 29 January 2015

[687] See http://europa.eu/rapid/press-release_IP-12-530_en.htm

[688] *Digital Rights Ireland v Minister of Communications & Ors* [2010] IEHC 221 at 113, 115(iii)

[689] *Tracey Cosgrove v Secretary of State for the Home Department*, CO/7701/2011

[690] Joined cases C-293/12 and C-594/12 *Digital Rights Ireland and Seitlinger and others* (Grand Chamber, 8 April 2004), 27

people concerned may lead to people considering that they are under constant surveillance.[691]

In determining the *necessity* of data retention, the Court stated that data retention did not 'adversely affect the essence'[692] of the rights granted by Art.7 of the Charter because content of communications was not retained. In addition, the Court recognised the need for States to fight crime and protect their citizens.[693] However, when verifying the *proportionality* of the interference to privacy created by data retention, the Court found that the EU legislature had a reduced level of discretion[694] and although data retention is an appropriate mechanism to aid in the fight against serious crime,[695] the mechanisms set out in the DRD may not, by themselves be a *necessary* measure.[696] On the issue of necessity, the Court also noted that the DRD interfered with the 'fundamental rights of practically the entire European population'[697] regardless of whether there is evidence that individuals are linked, even remotely to serious crime. The Court found major weakness in the limits to how retained data could be used and by whom, it being left to member States to determine the nature of serious crime and to set procedures for data access.[698] Moreover, the Court found that there was no judicial or independent review to limit the access to and use of data to what is strictly necessary for the fight against serious crime.[699] Furthermore, the Court was

---

[691] Ibid., 37

[692] Ibid. 39

[693] Ibid., 43-44

[694] Ibid., 48

[695] Ibid., 49

[696] Ibid., 51

[697] Ibid., 56

[698] Ibid., 60-61

[699] Ibid., 62

critical that the DRD did not require that retained data remain in the EU, potentially leading to breaches of data protection legislation.[700]

Although it accepted that the reasons for retaining metadata were genuinely to aid the fight against serious crime, the Court stated that the EU legislature had 'exceeded the limits imposed by compliance with the principle of proportionality.'[701] The Court found the DRD to be invalid. This was the first time an entire legal instrument had been declared invalid for breaching fundamental rights in the EU.[702]

This research has shown that the effect of the Court's declaration indicated, once again, just how far the UK government would go in its quest for such data. The Open Rights Group reported that a Swedish ISP deleted all its retained data, the Government of Finland announced a review indicating that it wishes to uphold the law, whereas the UK government introduced emergency legislation to permit it to continue to retain data.[703] This legislation was enacted as the Data Retention and Investigatory Powers Act, 2014 (DRIPA) which progressed from Bill to Royal Assent in just three days.[704]

However, DRIPA went further than simply permitting the continuation of data retention in the wake of the striking down of the Data Retention Directive. It expanded to the definition of telecommunication service in RIPA by adding the case where such a service included facilities to create, manage, store or

---

[700] Ibid., 68

[701] Ibid., 69

[702] Judith Rauhofer and Daithí Mac Síthigh, 'The Data Retention Directive Never Existed', Scr*ipte*d Volume 11, issue 1, April 2014, 119

[703] See https://wiki.openrightsgroup.org/wiki/Data_Retention_Directive#Result_of_ECJ_decision

[704] See http://services.parliament.uk/bills/2014-15/dataretentionandinvestigatorypowers/stages.html accessed 4/4/15

transmit a communication.[705] This makes it clear that services such as webmail are to be included.

The Government also included modifications to RIPA s.11 to enable warrants for interception to be served on people outside the UK which 'may relate to conduct'[706] outside the UK. Similarly, RIPA s.12 was modified to enable the UK to order extra-territorial companies to maintain the technical ability to assist with interception,[707] and to retain and disclose metadata.[708] As illustrated in this research, this effectively expanded the UK's intercept and data retention abilities globally.[709]

Section 21 of the Counter-Terrorism and Security Act 2015 (CTSA) modified DRIPA s.2(1) to specifically add the requirement to retain IP addresses.[710] DRIPA had a sunset clause revoking all sections on 31 December 2016.[711] Potentially, the only positive inclusion in DRIPA was the requirement to appoint an independent person who would review terrorism legislation and the operation of investigatory powers.[712]

Although clearly a stop-gap with a short sunset clause, DRIPA had a much shorter life than anticipated by the Government. On 17 July 2015, DRIPA s.1 was found to be inconsistent with EU law and was ordered to be disapplied. The Court found that DRIPA did not set clear rules for access and use of metadata, in particular there was no precise definition of what serious offences

---

[705] Data Retention and Investigatory Powers Act 2014 (DRIPA), s.5

[706] Ibid., s.4(2)

[707] Ibid., s.4(6)

[708] Ibid., s.4(8)

[709] Subhajit Basu and others, Open letter from UK internet law academics, <http://www.law.ed.ac.uk/__data/assets/pdf_file/0003/158070/Open_letter_UK_internet_law_academics.pdf> accessed 25 July 2014

[710] Counter-Terrorism and Security Act 2015 s.21(3)(b)

[711] DRIPA (n 705) s.8(3)

[712] Ibid., s.7

were in its scope.[713] The Court was also critical of the fact that metadata could be made available without prior review by a court or independent body which could place limits on how the data may be used.[714]

The Government had requested that the Court referred the case to the CJEU.[715] While declining, the Court noted that the sunset clause of DRIPA would make it unlikely to get a response from the CJEU in time.[716] The claimants had stated they did not wish DRIPA to fall without a suitable remedy.[717] The Court granted this by suspending the disapplication of DRIPA s.1 until 31 March 2016.[718] The Government appealed, but the Court of Appeals concluded that it had to refer the matter to the CJEU.[719] The outcome is further examined and presented in Chapter 7. Meanwhile, legislation to allow metadata retention to continue would come in the form of the Investigatory Powers Act and hence, this is discussed next.

4.5 The Investigatory Powers Act

Out of all the sometime complex legislation in force in the UK governing surveillance, when introducing the Investigatory Powers Bill to Parliament, the Home Secretary revealed that bulk metadata collection had been carried out under the direction of secretaries of state via Section 94 of the Telecommunications Act 1984 which simply permitted the government to

---

[713] *David Davis and others v Secretary of State for the Home Department* [2015] EWHC 2092 (Admin), 122

[714] ibid.

[715] Ibid., 104

[716] Ibid., 113

[717] Ibid., 117

[718] Ibid., 121

[719] Secretary of State for the Home Department v Davis MP & Ors, [2015] EWCA Civ 1185, 117-118

require providers to essentially do whatever they were asked.[720] This research found that the action was effectively undertaken in secret with only a few senior cabinet ministers being aware.[721]

With so much press involvement after Snowden and with the striking down of DRIPA, the Government had to take action to ensure it could continue to monitor Internet communications. There were three major reviews published in 2015. The Intelligence and Security Committee (ISC) of Parliament published a redacted version of its report in March 2015. In June 2015, the Independent Reviewer of Terrorism Legislation issued his report of the investigatory powers review (IPR). The Royal United Services Institute (RUSI) published its independent surveillance review (ISR) in July 2015. The ISC and ISR reports were both as a result of the Snowden revelations, whereas the ISR report was undertaken as required by DRIPA s.7.

Paying attention to the findings of all three reports, the UK Government published the draft Investigatory Powers Bill in November 2015. This Bill aimed to create one consolidated Act, incorporating bulk interception and acquisition of metadata both within the UK and overseas[722] while only seeking enhanced powers over metadata retention via the requirement to create and retain Internet Connection Records (ICRs)[723] which would be retained for 12 months.[724] However, despite this reassurance, the House of Commons

---

[720] HC Oral Answers 4 Nov 2015 at 971

[721] Nick Clegg, The surveillance bill is flawed but at least we have oversight, The Guardian, 5/Nov/15 <http://www.theguardian.com/commentisfree/2015/nov/05/surveillance-bill-mi5-secret-database> accessed 31 December 2015

[722] HC Oral Answers (n 720)

[723] Draft Investigatory Powers Bill, Foreword

[724] Draft Investigatory Powers Bill ,49

Science and Technology Committee found that the actual nature of ICRs were not made clear.[725]

The Investigatory Powers Act became law on 29 November 2016 and it repealed ATCSA Part 11 and CTSA s.21, both dealing with data retention, and all of DRIPA. It also repealed Part 1 of RIPA, and s.94 of the Telecommunications Act 1984. The various provision of these acts and sections were incorporated into the Act. On a positive note, the Act purports to set out how privacy may be invaded and protected. In this, it recognises that investigatory powers are privacy invasive.[726] There are improvements in oversight in the dual lock that requires a Judicial Commissioner to check any warrants. However, there is one wholly new provision in the Act which is examined next.

4.5.1 Communications data and Internet Connection Records

Section 87 defined relevant communications data as that data which may identify or assist in the identification of any of the following five categories:

1. 'the sender or recipient of a communication (whether or not a person)'[727]
2. 'the time or duration of a communication'[728]
3. 'the type, method or pattern, or fact, of communication'[729]
4. 'the telecommunication system (or any part of it) from, to or through which, or by means of which, a communication is or may be transmitted'[730]

---

[725] House of Commons Science and Technology Committee, Investigatory Powers Bill: technology issues, Third report of Session 2015-16, HC 573, p3

[726] Investigatory Powers Act 2016, s.1

[727] Ibid., s.87(11)(a)

[728] Ibid., s.87(11)(b)

[729] Ibid., s.87(11)(c)

[730] Ibid., s.87(11)(d)

5. ‘the location of any such system’[731]

The section notes that this specifically includes ICRs. By specifying *any part* of a telecommunication system and including non-persons in the definition of sender or recipient, it means that no part of the Internet is safe.

An ICR is defined as metadata which has two characteristics. First, it is data which ‘may be used to identify, or assist in identifying, a telecommunications service to which a communication is transmitted by means of a telecommunication system for the purpose of obtaining access to, or running, a computer file or computer program’.[732] Second, it is data ‘generated or processed by a telecommunications operator in the process of supplying the telecommunications service to the sender of the communication (whether or not a person)’.[733]

The definitions of telecommunications system and telecommunications service are the same as in RIPA s.2. However, the access and use clause of the latter is specifically defined as including the ability to create, manage or store a communication which has been or may be transmitted.[734] This would cover webmail systems.

Communications as related to the Internet are defined as data of any form and the signals that carry a communication between entities,[735] whereas an entity being defined as a ‘person or thing’.[736] As written, this would appear to be all encompassing including communications between Internet devices, routers, for instance, and IoT devices. Communications data is split into entity data

---

[731] Ibid., s.87(11)(e)

[732] Ibid., s.62(7)(a)

[733] Ibid., s.62(7)(b)

[734] Ibid., s.261(12)

[735] Ibid., s.261(2)

[736] Ibid., s.261(7)

and events data. Events data refers to the timing of a communication,[737] while entity data is data about an entity or its association with a telecommunications service or system and can identify or describe the entity, potentially including its location.[738]

Communications data is defined as consisting of:

- data about an entity that a service has been provided to and relates to the provision of that service;[739]
- data which is necessary to enable a communication to take place;[740]
- data relating to the use of a telecommunication system or service;[741]
- data about the architecture of the system which is not about a specific person.[742]

Some potential examples were listed in the Communications Data Draft Code of Practice issued in August 2016.[743] It is expected that this data will be held by a telecommunications operator directly or held on their behalf, or that the capability to hold this data exists or could exist.[744] In the case of data necessary to enable a communication, this may also be available directly from the telecommunication system.[745]

---

[737] Ibid., s.261(4)

[738] Ibid., s.261(3)

[739] Ibid., s.261(5)(a)(i)

[740] Ibid., s.261(5)(a)(ii)

[741] Ibid., s.261(5)(a)(iii)

[742] Ibid., s.261(5)(c)

[743] Home Office, Communications Data Draft Code of Practice, August, 2016 <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/557862/IP_Bill_-_Draft_CD_code_of_practice.pdf> accessed 14 December 2016

[744] Investigatory Powers Act (n 726) s.261(5)(a)

[745] Ibid., s.261(5)(b)

The creation and retention of ICRs have the potential to create a vast amount of data. Desktop PCs and mobile devices continually make connections to services. CG-NAT, Web accelerators and browser pre-fetching all further complicate the issue. Because of this, the ICRs become a record of what the device was doing, not what the user was doing. Recording information in this way not only records which servers a device connects to, but also it could be used to indicate what apps are installed on that device, further invading the owner's privacy. Even if ICRs prove feasible, there are major issues. Use of publically-available Wi-Fi, for example, in a hotel or surgery where no initial sign-up is required will mean there is no data as to who a user may be. Someone routing through a Virtual Private Network (VPN) in a foreign jurisdiction will place their onward connections out of the reach of the Act.[746] Had the Act simply specified that an ISP must be able to determine who accessed what server or service and when, then the ISP can then work out the best mechanism to do so and adjust that method as technologies change.[747]

Towards the end of 2016, the Investigatory Powers Act became the latest in a series of legislation whose primary aim is to enable surveillance. On one hand, the Act has had a great deal of scrutiny and this has been carried out with the full inclusion of CSPs and other providers. Scrutiny will continue via the Investigatory Powers Commission. On the other hand, by introducing ICRs, it reveals just how far the government wants to go in order to legitimise existing and enable new ways to invade Internet privacy.

---

[746] House of Lords, House of Commons, Joint Committee on the Draft Investigatory Powers Bill report, HL Paper 93, HC 651, 3/2/16, at 132-133

[747] House of Lords, House of Commons, Joint Committee on the Draft Investigatory Powers Bill: Written Evidence, Richard Clayton written evidence (IPB0032)

4.6 Conclusion

This chapter demonstrated how the UK has had to implement laws due to unfavourable court decisions of the ECtHR which found that the UKs surveillance was not lawfully defined. It can be seen that the Government has not readily legislated on or provided proper control of such surveillance until there was no other option but to introduce legislation. As illustrated in this chapter, the *Malone* case, and then other ECtHR cases have had a very significant effect on surveillance laws in the UK. The UK has laws dealing with data protection, but these give no real protection from the State. It has laws regulating surveillance, but these have developed in order to protect the Government in an international context rather than as a benefit to the people. The result as shown in this research is that current online privacy comes from a 'hodgepodge of laws and the side-effect of complex regulations'[748] and yet, in other complex areas, the existing laws have been codified into simple acts such as the Theft Act and Fraud Act.

Like the US, the UK has faced a cycle of legislative changes followed by changes in technology outdating those laws. However, unlike the US which has scaled back some of its most intrusive surveillance programmes the UK has now implemented what has been described by Snowden as 'the most extreme surveillance in the history of western democracy [going] farther than many autocracies'.[749] When comparing the US and the UK, the UK must take the lead in the eradication of Internet privacy. While the previous chapter concluded that Internet privacy is not yet lost in the US it is much closer to death in the UK due to the introduction of the Investigatory Powers Act and ICRs. While these are new and it is as yet uncertain exactly how they will be implemented the ability to record and store for future use the

---

[748] All Party Parliamentary Communications Group (n 313) 149 to 151

[749] Edward Snowden (*Twitter*, 17 November 2016) <https://twitter.com/i/web/status/799371508808302596> accessed 25 January 2017

browsing habits of the entire population can only be seen as the loss of Internet privacy in the UK.

After reviewing the extent to which Internet privacy is affected by communications surveillance legislation and practices within the US and the UK, the focus is now turned to China. This is because China has been viewed by the West as an autocratic institution which attempts to control its population using various means including a country-wide firewall and Internet monitoring system. Many people will think that Internet privacy is non-existent in China. So, the question is how different, or indeed if, the US and the UK really are from the situation as we see it in China. This becomes the focus of the discussion in the next chapter.

Chapter 5: China, its Internet and its surveillance

5.1 Introduction

The previous two chapters provide a detailed, in-depth analysis of the level and status of Internet privacy in the contexts of the US and the UK. One of the significant research findings is that communications surveillance has been highlighted as a precursor to invasion of Internet privacy. Additionally, the situation in the US and the UK was shown to be biased against Internet privacy, heavily so in the case of the UK since the passage of the Investigatory Powers Act at the end of 2016.

However, in China, the telecommunications infrastructure did not begin to develop in earnest until after 1980. Prior to this time, telecommunications were viewed mainly as a state or military system and used for bureaucratic purposes. By 1980, the penetration of telephones was only 0.43%.[750] China's criminal law as amended in 1997 still did not consider telecommunications, referring only to the unlawful opening of letters as invasive of a person's right to freedom of correspondence.[751] Thus, there was no law criminalising the interception of communications or, indeed, mentioning the subject in any way.

The aim of this chapter is to investigate whether Internet privacy exists, or indeed can exist in China, in particular given its tight level of control over its national Internet and the flow of information to and from the rest of the global Internet.

---

[750] Zhenzhi Gou and Mei Wu, 'Dancing thumbs: Mobile telephony in contemporary China', in Xiaoling Zhang and Yongnian Zheng, (Eds.) *China's Information and Communications Technology Revolution: Social changes and state responses* (Routledge, Abingdon 2009) p39

[751] Criminal Law (n 225) Art. 252

5.2 Regulation of the Internet in China

China acted quickly to introduce legislation that required that all computer systems which had international access were to be registered.[752] It promulgated interim provisions in February 1996[753] which stated the requirement that any network in China that was to have an international connection would use such a connection provided by the MPT;[754] otherwise, it was not permitted to establish an international connection.[755] Networks would be connected via an interconnection network[756] of which four were defined as being run by the MPT, the Ministry of Electricity Industry (MEI), the State Commission of Education and China Science Academy.[757] They also required that users must be registered,[758] and stated that international networks must not be used for illegal activities or those which would damage social order or national security. Access to pornography was also banned.[759]

The interim provisions were followed two months later in April 1996 by another set of regulations dealing specifically with the public network - Chinanet.

---

[752] Regulations of the People's Republic of China for Safety Protection of Computer Information Systems, promulgated by Decree No. 147 of the State Council of the People's Republic of China and effective as of February 18,1994, Art.11

[753] Interim Provisions Governing the Management of the Computer Information Networks in the People's Republic of China Connecting to the International Network, adopted at the 42nd Executive Meeting of the State Council on January 23, 1996, promulgated by Decree No. 195 of the State Council of the People's Republic of China on February 1, 1996

[754] Ibid., Art.6

[755] Ibid., Art.6

[756] Ibid., Art.8

[757] Ibid., Art.7

[758] Ibid., Art.10

[759] Ibid., Art.13

These regulations included the need to cooperate with State monitoring.[760] Moreover, the regulations imposed the duty to report infringements[761] as well as the duty to not infringe other people's legal rights.[762] By now, China had a functional Internet with international connections and was finding ways to at least discover what the networks were being used for.

The requirement to gain a licence to connect to international networks was added in 1997 when the 1996 interim provisions were updated.[763] Evidently, this was a purposeful move by China as licences can be revoked, which would result in the relevant provider being effectively cut off from the global Internet.

5.2.1 Laws and regulations governing the Internet

China's development of the Internet combines both expansion and management. It aims to constantly develop methods to manage the Internet 'in accordance with the law'[764] to protect 'social stability and state security.'[765] Nevertheless, China's approach tends to be to implement laws and

---

[760] Measures on the Regulation of Public Computer Networks and the Internet, promulgated by the Ministry of Posts and Telecommunications on April 9, 1996, Art. 12

[761] Ibid., Art. 10

[762] Ibid., Art. 11

[763] Interim Provisions Governing the Management of the Computer Information Networks in the People's Republic of China Connecting to the International Network, promulgated by Decree No. 195 of the State Council of the People's Republic of China on February 1, 1996, and revised in accordance with the Decision of the State Council Regarding the Revision of the Interim Provisions Governing the Management of the Computer Information Networks in the People's Republic of China Connecting to the International Network, promulgated on May 20, 1997, Art. 8

[764] Wang Chen, Concerning the development and administration of our country's Internet, (HRIC tr.) I (3) <http://www.hrichina.org/crf/article/3242> accessed 4 October 2011. Note this is a translation of the speech as published on 4 May 2010 which was later heavily edited and replaced the next day. p24

[765] Ibid.

regulations which are both complex and, sometimes, overlapping, making it increasingly hard to understand right from wrong.[766] The many government entities which have an interest in the Internet resulted in numerous laws being drafted. These laws are in some cases never enforced, or worse are in conflict with one another. However, they do provide the maximum level of control.[767]

In 1997, China promulgated the Computer Information Network and Internet Security, Protection and Management Regulations.[768] Art. 3 of these Regulations charged the Computer Management and Supervision Bureau (CMSB) of the Ministry of Public Security (MSP) with maintaining the physical and online security of China's computer networks. Art. 4 of the Regulations prohibits the use the Internet to disclose state secrets or harm national security, or to harm the interests of China, its society, groups or individuals. Criminal activity on the Internet is also prohibited.[769]

Art. 5 defines several prohibited categories of information and it is not permitted to create, copy, transmit or even to retrieve information which falls into any of the following categories:

(1) Inciting to resist or breaking the Constitution or laws or the implementation of administrative regulations;
(2) Inciting to overthrow the government or the socialist system;
(3) Inciting division of the country, harming national unification;
(4) Inciting hatred or discrimination among nationalities or harming the unity of the nationalities;

---

[766] Cullen and Choy (n 298) 132

[767] Nina Hachigian, 'China's Cyber–Strategy', 80 Foreign Aff. 118 2001, p123

[768] Computer Information Network and Internet Security, Protection and Management Regulations, approved by the State Council on December 11, 1997 and promulgated by the Ministry of Public Security on December 30, 1997, Art. 3

[769] Ibid., Art. 4

(5) Making falsehoods or distorting the truth, spreading rumours, destroying the order of society;
(6) Promoting feudal superstitions, sexually suggestive material, gambling, violence, murder;
(7) Terrorism or inciting others to criminal activity; openly insulting other people or distorting the truth to slander people;
(8) Injuring the reputation of state organs;
(9) Other activities against the Constitution, laws or administrative regulations.[770]

Furthermore, Art. 6 covers harm to China's Internet itself, for example by introducing computer viruses or deleting or altering information in transit.[771] Finally, Art. 7, which is the most important of all, states that the freedom and privacy of Internet users is legally protected.[772]

Regulation of ISPs was equally strict. For instance, Art. 8 states that ISPs must assist the Public Security Bureau (PSB) by discovering and handling violations.[773] If a violation of Arts. 4, 5, 6 or 7 of the Regulations is discovered, the information concerned must be preserved in an unaltered form and reported to the local PSB,[774] and more specifically for breaches of Art. 5, the relevant server is to be removed from the network.[775] Because of the fines and potential criminal prosecution for failures to comply with the duties set out by the Regulations,[776] ISPs implemented policies for self-censorship and

---

[770] Ibid., Art. 5

[771] Ibid., Art. 6

[772] Ibid., Art. 7

[773] Ibid., Art. 8

[774] Ibid., Art. 10(6)

[775] Ibid., Art. 10(7)

[776] Ibid., Art. 20-23

employed staff to supervise potentially large groups of volunteers who policed and cleaned bulletin boards and chatrooms.[777]

Overarching Internet rules were implemented in 2000 by a Decision of the National People's Congress (NPC) Standing Committee. China's Internet laws are generally based on general laws; however, the Decision made it clear that while violations of people's rights would result in civil liability,[778] where an action was a crime, it would be prosecuted under the relevant provision in the criminal code.[779] Furthermore, actions in violation of public order which are not specifically crimes would result in penalties levied by public security organs or administrative departments.[780]

The Decision set out specific violations regarding the use of the Internet. Of these, several are relevant to this research such as the spreading of rumours, slander, subversion and harm to the socialist system or the undermining of national unity; theft and publication of state, intelligence or military secrets; ethnic hatred; and the setting up of or communication with evil cults are all violations presenting a danger to national security and social stability.[781] Detecting such violations requires surveillance and monitoring to the detriment of Internet privacy.

The publication of or provision of access to pornography is also a violation,[782] as is the use of the Internet to insult or slander others,[783] or to commit 'theft,

---

[777] International Centre for Human Rights and Democratic Development, Review of China's Internet Regulations and Domestic Legislation

[778] Ninth National People's Congress Standing Committee: Decision of the National People's Congress Standing Committee on Safeguarding Internet Security 1-5

[779] Ibid., (unnumbered)

[780] Ibid., 6

[781] Ibid., 2

[782] Ibid., 3(5)

[783] Ibid., 4(1)

fraud or extortion'.[784] Additionally, modification or deletion of another person's e-mail or other data, and intrusion into a person's 'civil freedoms and confidentiality of correspondence'[785] are violations. This last point suggests there may be some protection of Internet privacy at a personal level, but not against the State.

The wording of the Decision is designed to be future-proof. Where an action does not fall into one of the categories outlined above but does constitute a crime, then it too will be dealt with under the relevant criminal code.[786] The requirements set out in the Decision would filter down into all subsequent Internet-related laws and regulations.

Regulation of pornography was particularly strict, criminalising not only the production of such material but also the act of knowingly linking to it.[787] The policing of pornography is a burden placed on all citizens, a person was also guilty of a crime if they were aware that others were dealing with obscene material but failed to report it.[788]

As found in this research, there is some protection for people's rights on the Internet in China. Regulations promulgated in 1997 made it an offence to use the Internet to violate the privacy and freedom of users.[789] In addition,

---

[784] Ibid., 4(3)

[785] Ibid., 4(2)

[786] Ibid., 5

[787] Explanations of a Number of Issues in the Specific Application of the Law on Handling Criminal Cases of Using the Internet, Mobile Communications Terminals, and Voice Sets for the Production, Reproduction, Publication, Sale, and Dissemination of Obscene Electronic Information, 6th September, 2004, Art. 4

[788] Ibid., Art. 7

[789] Computer Information Network and Internet Security, Protection and Management Regulations, approved by the State Council on December 11, 1997 and promulgated by the Ministry of Public Security on December 30, 1997.

publishing 'contents that … infringe upon other people's legitimate rights'[790] on a bulletin board system is an offence. It is similarly an offence for Internet information service providers,[791] Internet news and information services[792] and providers of Internet cultural products.[793]

Furthermore, e-mail messages get specific confidentiality protection, exceptions being for national security or tracing crime.[794] E-mail providers are also required to keep users' registration and e-mail addresses confidential.[795]

China's desire to control information is further illustrated by regulations applied to Internet news services in 2005. The regulations stipulate that services publishing political or current affairs news to the public must not alter the original official news material. Furthermore, services set up in order to republish existing material are not permitted to create their own material.[796]

George W. Bush, then governor of Texas said: 'Imagine if the Internet took hold in China. Imagine how freedom would spread.'[797] However, freedom as

---

[790] Ministry of Information Industry, Regulations on the Management of Internet Electronic Bulletin Services, Art. 9(8)

[791] State Council, Measures for the Management of Internet Information Services, Art. 15(8)

[792] Ministry of Information Industry, Regulations on the Management of Internet News and Information Services, Art. 19(8)

[793] Ministry of Culture, Interim Regulations on the Management of Internet Culture, Art. 17(8); Internet cultural products refer to audiovisual products, games, dramatic shows, works of art, animations and other such products, see Art. 2 of the Interim Regulations.

[794] Measures for the Management of Internet E-mail services, Art. 3

[795] Ibid., Art. 9

[796] Regulations on the Management of Internet News and Information Services, Art. 16

[797] Republican presidential candidates debate in Phoenix, Arizona, December 6th 1999 <http://www.presidency.ucsb.edu/ws/index.php?pid=75089> accessed 24 September 2011

a Western construct did not spread as a result. This research found that China has managed to create an Internet infrastructure which permits a great deal of control. It's Internet laws set out clearly that, while there may be some protection of privacy at an interpersonal level, there is little protection from the State. Additionally, providers are given the responsibility of policing the Internet and reporting violations. In order to do so they form an army of censors and monitors keeping watch over what citizens are doing on the Internet. Last but not least, the Internet structure China created allowed it to build a country-wide firewall and filtering system which sits between China and the rest of the global Internet. This is discussed in the next section.

5.3 Controlling the Internet: Golden shield

China's Golden Shield is one of a series of 'Golden' projects which were China's 'telecommunication and information infrastructure initiatives'[798] of the 1990s. They consisted of projects to build the network infrastructure, implement e-Commerce and provide information to China's leaders.[799]

Golden Shield is a public security and surveillance system which encompasses a full range of monitoring technologies from telephone to Internet.[800] In part, it aims to stop Internet crime, guarantee the security of the public Internet and combat groups such as Falun Gong.[801]

The name Golden Shield has become synonymous with the Great Firewall of China; the Firewall is only one component of the whole Shield, yet it still has great significance on influencing Internet privacy in China.

---

[798] Walton (n 300) 17

[799] Ibid., box 2 at p17

[800] Ibid., 17

[801] Cisco Public Security Sector slides p57 – the slide notes that this information was from a statement of government goals from a speech by Li Runsen.

5.3.1 Technical censorship

In a speech in 2000 former US President Bill Clinton questioned how much the Internet could change China. He commented that although China was attempting to control the Internet it was 'sort of like trying to nail Jello to the wall'.[802] Despite this, China has, in fact, done just that. China 'devoted extensive resources'[803] to build what became 'one of the largest and most sophisticated'[804] Internet content filtering and blocking systems in the world. It has become known as the Great Firewall of China.

Because of the way its Internet has been constructed, it is relatively easy for China to impose this total control. The system allows China to 'physically monitor all traffic into or out of the country'[805] and also to forward its own cause.[806]

The system works in two ways: it uses an IP address block list and also a list of forbidden keywords. The former is the simplest way because the system can simply drop connections where the destination IP address matches one on the list. However, keyword checking requires the use of DPI because the information exists within the content part of the packet. Further explanations of DPI are given in Chapter 6. The system checks words in URLs against the forbidden list and can terminate the connection if a match is found. Thus,

---

[802] Speech by Bill Clinton at the Paul H. Nitze School of Advanced International Studies, Washington D.C., Mach 8, 2000 <http://usinfo.org/wf-archive/2000/000380/epf302.htm> accessed 25 April 2011

[803] OpenNet Initiative, *Internet filtering in China in 2004-2005: A Country Study*, 1

[804] Ibid.

[805] James Fallows, 'The connection has been reset' (*The Atlantic*, March 2008) <http://www.theatlantic.com/magazine/archive/2008/03/the-connection-has-been-reset/306650/> accessed 24 September 2011

[806] Yongnian Zheng, *Technological Empowerment: The Internet, State, and Society in China* (Stanford University Press, 2008) xv

taking ‘falungong’[807] as an example of a blocked word, any URL containing the string ‘falungong’ would be blocked. This same mechanism will block searches via search engines as the search terms will appear in the URL string being requested.

Encryption can prevent access to the data, but the Firewall blocks access to Google’s encrypted search.[808] In addition, the firewall can also block any form of encrypted connection, ensuring that data passing across it remains in clear text and therefore, subject to interception.[809] Hence, there is a significant impact on Internet privacy in China.

As one may expect the keyword blocking system handles Chinese characters. However, it is found that it is prone to over block. For instance, in 2010, the word ‘carrot’ was blocked as one of the Chinese characters which makes the word is the same as the surname of President Hú Jǐntāo;[810] the filters are set to trap searches for the names of China’s leaders.[811]

On one hand, this kind of firewall may be viewed simply as a very large scale implementation of the blocking systems often found on school networks in the

---

[807] Falun Gong, or Falun Dafa is described as the ancient practice of self refinement and is heavily censored by China. Falun Gong was made illegal in China after protests in 1999; see for example http://www.falungong.org.uk/ accessed 24/sep/2011

[808] Google operates a website https://encrypted.google.com/ which would be encrypted end to end. If this were available in China the search terms passed from the user’s browser, and the returned search results could not be scanned for keywords by the firewall.

[809] The Enemies of the Internet: special edition : surveillance – China <http://surveillance.rsf.org/en/china/> accessed 09 December 2016

[810] Carrot - Húluóbo (胡萝卜); Hú Jǐntāo (胡锦涛)

[811] Michael Wines, Sharon LaFraniere and Jonathan Ansfield, ‘China’s censors tackle and trip over the Internet’, (*New York Times*, 7 April 2010) <http://www.nytimes.com/2010/04/08/world/asia/08censor.html> accessed 7 October 2011

UK[812]. However, it is also a national surveillance system and users who are constantly trying to reach blocked resources may well attract the attention of the security authorities.[813]

The Firewall is, however, generally located between the Internet in China and the rest of the world.[814] Its aim is to prevent people in China from accessing material held outside of China rather than controlling access within the country. For example, human rights material that is published by the China Society for Human Rights Studies[815] via a website within China is freely accessible. Nevertheless, even if this material is accessed via an external agent such as Google reader, the results are blocked by the Firewall as the pass through it.[816]

One major advantage of the filtering system is the ability to get people to view only the information China wants them to see. Bias can be created by forcing people to use China's own search engine, Baido. For example, a search on Google for many human rights topics will be blocked, yet a search on China's

---

[812] See for example the UK Safer Internet Centre's Appropriate Filtering and Monitoring guidance <https://www.saferinternet.org.uk/advice-centre/teachers-and-professionals/appropriate-filtering-and-monitoring> accessed 13 January 2017

[813] Fallows (n 805)

[814] A study published in 2011 determined there was some filtering capability within China but the majority was located at the border routers. See X Xu, M Mao and A Halderman, 'Internet censorship in China: where does the filtering occur?', in N Spring and G Riley, (eds.) *Passive and Active Measurement: 12th International Conference*, PAM 2011 LNCS 6579 (Springer, Berlin, 2011) pp 133-142

[815] See http://www.chinahumanrights.org/. This web server is located in Beijing (verified 24/Sep/2011)

[816] This was observed during a trip to Beijing. Google Reader takes RSS feeds from websites and presents these in a single web interface. However, as Google Reader runs on systems in the US, the returned data enters China via the firewall as is blocked, whereas direct access to the website from inside China is not blocked. As the www.chinahumanrights.org website is accessible from outside China, it means the firewall does not block outgoing material.

own search provider, Baido will not be blocked, nor will any of the news agency websites within China. Most people will attempt to find information elsewhere if their first choice of search engine is blocked,[817] and most people are only interested in information about their own country.[818] Baido itself will not index external, blocked content; thus, when users turn to Baido they will see heavily controlled sources of information, biased in favour of the state.[819]

Evidently, as explained above, the Great Firewall acts as a controller of information and a country-wide surveillance system which has significant influence on Internet privacy in China. Furthermore, in this research, it has been found that there has been much criticism of Western companies for supplying the equipment to China in the first place. Regardless of thoughts of right or wrong, China is such an important market that companies supplying equipment take a commercial decision to put profits first 'even at the risk of overlooking human rights.'[820]

The effects of the Firewall are varied. Although Facebook and Youtube are permanently blocked China has its own popular social media blogging site in Weibo. The majority of external websites and other Internet services remain accessible.[821] Furthermore, China's attempts to block pornographic websites are not abhorrent.

---

[817] Jonathan Zittrain, *The future of the Internet and how to stop it* (Yale University Press, New Haven, 2008) p105

[818] Fallows (n 805)

[819] This can be proved by simple experiment. While outside China, putting the phrase 'human rights in china' into Baidu finds main state-sponsored results, for example from China Daily. Putting the same phrase into Google finds the blocked Human Rights In China website as well as sites discussing rights abuses. (checked 25/sep/2011)

[820] Charles Li, 'Internet Content Control in China', 8 Int'l J. Comm. L. & Pol'y. 1, p27

[821] Experiments in Beijing showed that Facebook and Youtube were blocked permanently. However, there was no interruption to access to any University of Leeds website, the BBC websites, Google etc. including Google Mail.

5.3.2 Internet monitoring and surveillance

As the effectiveness of the firewall declines due to an increase in traffic, a logical solution for China is to move content filtering from the border gateways to homes and offices.[822]

In 2009, the MIIT announced its intention that all new PCs sold in China would have a software package pre-loaded known as Green Dam Youth Escort. A concern with this kind of software is that it may contain mechanisms to report back on what URLs have been attempted, thus moving surveillance into the home.[823] However, although Green Dam was not rolled out generally due to problems, it is still used in schools and cybercafés in China.

In addition to Green Dam Youth Escort, seemingly benign software can also be used to monitor online activity. For example, TOM-Skype, the Chinese version of Skype provided by TOM Online, was discovered to record the text of chat messages where these contained certain keywords relating to sensitive issues in China.[824] This practice would seem to be in line with China's law regarding the reporting of infringing content.

It is important to realise that unlike the US and the UK where the Internet is effectively provided by and operated by private companies, the Chinese government operates the backbone networks and has a controlling interest in the IAPs and gateways that connect it to the rest of the global Internet.[825] In

---

[822] Walton (n 300) 20

[823] Robert Farris, Hal Roberts and Stephanie Wang, 'China's Green Dam: the implications of government control encroaching on the home PC', (OpenNet Initiative Bulletin, undated), 18

[824] Nart Villeneuve, 'Breaching trust: An analysis of surveillance and security practices on China's TOM-Skype platform, Information Warfare Monitor / ONI Asia Joint Report' <http://www.nartv.org/mirror/breachingtrust.pdf> accessed 31 March 2016) (note the original URL as published in the document is no longer valid)

[825] David Kurt Herold, 'An inter-nation-al Internet: China's contribution to global Internet governance?' <http://ssrn.com/abstract=1922725> accessed 16 February 2016, 5

2002, Amnesty International reported that there were '30,000 state security personnel'[826] monitoring websites, chat rooms and e-mails. Hence, one may wonder what the level and magnitude of communications surveillance actually are in China.

To make matters worse, the research also found that metadata retention is a requirement in China. ISPs must keep a record of users' time online, URLs visited, and their account and telephone numbers[827] for 60 days and make the data available when required by law.[828] Premises established to provide Internet access such as cybercafés gained regulations in 2002, which specified that they must check and also record the identification cards or other credentials of customers as well as recording their login information. Once again, this data was to be kept for 60 days and made available on request.[829]

Unrestricted cybercafés often allowed anonymous access for citizens but China plans to eliminate stand-alone cybercafés by 2016, replacing these with regulated chains.[830] With the demise of these facilities it is not easy to use the Internet in China anonymously. So, once again, it leads one to wonder to what extent Internet privacy exists in China.

Worse still, Internet Content Providers (ICPs) are also expected to police the Internet. Content which spreads ethnic hatred, pornography, gambling or illegal acts, or damages social order or stability or the state itself are banned.[831] On finding such content, it is to be blocked, preserved and reported

---

[826] Amnesty International, People's Republic of China: state control of the Internet in China, (Amnesty International, 2002, ASA 17/007/2002) p2

[827] Measures for the Management of Internet Information Services Art. 14

[828] Ibid.

[829] Regulations on Administration of Business Premises for Internet Access Services, Art. 23

[830] China Media Bulletin, issue 6 January 20 2011, 'Stand-alone cybercafes to be eliminated in China by 2016'

[831] Measures for the Management of Internet Information Services Art. 15(6)

to the authorities.[832] Operators of electronic bulletin services, which includes bulletin boards, chatrooms and other interactive systems[833] have a similar duty as above to record user details[834] and report infringements.[835] Despite all these, ICPs also have a duty to keep the personal details of their users confidential, unless the user consents to disclosure or some other provision of law requires disclosure.[836] Internet news services carry the same content reporting requirements[837] and such services also include blogs. The evolution of Web 2.0 has placed a 'higher demand on Internet users to abide by the law and learn to discipline themselves.'[838]

The content of e-mails[839] is subject to China's telecommunications regulations which prohibit contents that 'spread rumours, disturb social order, or undermine social stability'.[840] ISPs must record e-mail addresses, IP numbers and times of messages sent through their relays for 60 days.[841] In addition, e-mail providers must respond to reports of prohibited content. Reports were to

---

[832] Ibid., Art. 16

[833] Regulations on the Management of Internet Electronic Bulletin Services Art. 2

[834] Ibid., Arts. 14-15

[835] Ibid., Art. 13

[836] Ibid., Art. 12

[837] Regulations on the Management of Internet News and Information Services, Art. 19

[838] Chen (n 764) 24, 30-31

[839] Ministry of Information Industry, Measures for the Management of Internet E-mail Services, Art. 11

[840] Regulation concerning Telecommunications of the People's Republic of China, Art. 57(8)

[841] Ministry of Information Industry, Measures for the Management of Internet E-mail services, Art. 10

be passed to a handling unit operated by the China Internet Association on behalf of the MII.[842]

5.3.3 Enforcement

Although information is scarce there is evidence of the effectiveness of the monitoring and filtering outlined above. Below are depicted some supporting cases for this.

Lin Hai became the first person to be sentenced specifically for an Internet crime in 1998. He was accused of sending the e-mail addresses of some 30,000 Chinese citizens to a US pro-democracy magazine.[843]

In 2001, Huang Qi[844] became the first person in China to be tried for posting human rights articles.[845] In 2002, student Liu Di was arrested for posting material on the web, persuading others to protest at the arrest of Huang Qi. As a result, thousands of people signed an online petition for her release. She was not known as a dissident, simply being someone who posted her thoughts online.[846] She was released in November 2003 on bail.[847]

This, and other similar cases, is, perhaps, unsurprising in a country where a 'sophisticated security apparatus monitors what citizens read and write online.'[848] Amnesty International reported that it believed 54 people were in

---

[842] Ibid., Art. 15

[843] Cullen and Choy (n 298) p127

[844] Huang Qi is a human rights activist. He runs a website known as Tian Wang, now hosted on a server in the USA and blocked from access from within China. See http://64tianwang.com accessed 9/oct/11

[845] Amnesty International, People's Republic of China: controls tighten as Internet activism grows, (Amnesty International, 2004, ASA 17/001/2004) p3

[846] Ibid., p5

[847] Zheng (n 806) p127

[848] Ibid.

detention in China for Internet-related offences, with prison sentences ranging from 2 to 12 years.[849] In many cases this has involved people downloading and disseminating or writing material online about sensitive or banned topics; for example, 17 people were jailed for discussing Falun Gong and 16 for discussing the democracy movement.[850] The Amnesty International report includes the names of a further four people arrested for Internet offences who died in custody.[851] It is clear that most cases relate to freedom of expression rather than privacy. Openly posting material online shows little expectation of privacy by the individual concerned. However, the Amnesty International list includes four people arrested for signing the online petition or posting articles demanding the release of Liu Di.[852] One of these four[853] posted under a pseudonym, and it would be reasonable to assume this person did so to attempt to maintain privacy.

Up until now, the research findings have shown that Internet law in China is both complex and strict, and its effects can be extreme; for instance, in 1998, two brothers found guilty of hacking into a bank database were sentenced to death.[854]

In addition to severe penalties, the mere fact that one's actions online can easily be monitored creates a very chilling effect and as a result, it promotes

---

[849] Amnesty International, People's Republic of China: controls tighten as Internet activism grows, (Amnesty International, 2004, ASA 17/001/2004), 2

[850] In addition to the 54, the Amnesty International report lists a further four Chen Quilan, Li Changjun, Xue Hairong and Zhao Cahunyin, all Falun Gong supporters or practitioners, who died in custody. See Appendix II of the Amnesty International 2004 report (AI 17/001/2004)

[851] Amnesty International (n 849) p35

[852] Cai Lujun (also wrote essays calling for democratic reforms), Du Daobin (also posted about social and political issues), Kong Youping (also posted articles about the 1989 uprising), and Lou Changfu.

[853] Lou Changfu posted using the pseudonym 'Justice add Consciousness'

[854] Cullen and Choy (n 298) 128

and enforces self-censorship by individuals, ICPs and ISPs alike. Nevertheless, this is self-censorship by fear. Mobilising agents to find and arrest individuals found to be in breach of China's Internet laws serves as a warning to others. The vagueness of the laws themselves makes people over cautious.[855] As a result, from this research, it would seem that in China, the only way to protect one's Internet privacy is to not use the Internet.[856]

In fact, the effects of self-censorship have gone further than the aforementioned and some implications are worth noting. For instance, western companies providing search engine facilities became a part of this overall censorship. Yahoo!, Microsoft and Google all altered their products in order to filter keywords or close down blogs.[857] Yahoo! would go further. The trial in 2005 of Shi Tao was widely reported at the time. Shi Tao was the director of a newspaper news and editorial department and had been briefed on state secrets in confidence. He emailed information about the briefing to an editor acquaintance in New York asking that the information be quickly disseminated. The Court heard that Shi Tao had used his personal Yahoo! e-mail account. The authorities had obtained a copy of the e-mail and Yahoo! Hong Kong had provided the IP address and corresponding information tying this to the newspaper's telephone line user for dial-up Internet access. Shi Tao was sentenced to 10 years imprisonment and a further 2 years loss of political rights.[858]

---

[855] Kissel (n 299) 244-245

[856] Shaojung Sharon Wang and Junhao Hong, 'Discourse behind the Forbidden Realm: Internet surveillance and its implications on China's blogosphere', Telematics and Informatics 27 (2010) 67-78, 74

[857] Miriam D D'Jaen, Breaching the Great Firewall of China: Congress Overreaches in Attacking Chinese Internet Censorship, 31 Seattle U. L. Rev. 327 2007-2008, pp332-334

[858] Changsha Intermediate People's Court's Written Judgment in the Shi Tao State Secrets Trial <http://www.cecc.gov/publications/commission-analysis/changsha-internediate-peoples-courts-written-judgment-in-the-shi> accessed 20 March 2016

5.4 Data protection in China

In 2001, elements of data protection were written into China's criminal law.[859] Art. 253a states that anyone who illegally obtains personal information will, if the offence is serious enough be sentenced to up to 3 years in prison and/or fined. On 5 January 2010, Zhou was prosecuted under the amended law for his role in a 'data scam'[860] in what was reported as the 'first-known case of violating the security of personal information'.[861] He obtained the phone numbers of 14 government officials via his private investigation company and sold these to a scammer. He was sentenced to 1.5 years in prison.

New guidelines aimed at the protection of personal information took effect on 1 February 2013.[862] These appear to attempt to implement many of the protections present in EU data protection law. For example, it includes the principle of informed consent,[863] confidentiality,[864] the right to know what data is held about oneself,[865] and the right to have data corrected.[866] There is clearly a change in China towards the protection of personal information.

---

[859] Criminal Law of the People's Republic of China as amended by Amendment 7 on February 28th, 2009

[860] Quanlin Qui, 'Personal data scam, 8 jailed' (*China Daily*, 01/05/2010) <http://www.chinadaily.com.cn/cndy/2010-01/05/content_9263566.htm> accessed 23 March 2016; note the news item incorrectly states the Article as 7 whereas it is Article 253a.

[861] Ibid.

[862] Information Security Technology – Guidelines for Personal Information Protection Within Public and Commercial Services Information Systems

[863] Ibid., 3.7

[864] Ibid., 4.2

[865] Ibid., 4.3

[866] Ibid., 4.5

In 2012 the NPC Standing Committee issued a Decision that aims to protect personal information including that which involves an individual's privacy.[867] The Decision deals generally with data protection and provides a suitable framework, requiring, for example that providers state what personal information they are gathering, why, and how it will be used, and ensuring they will keep personal information confidential.[868]

5.5 Internet privacy in China

Westin finds that anonymity is one of the cornerstones of privacy and provides 'freedom from identification and surveillance'.[869] However, online anonymity in China is becoming increasingly difficult to achieve.[870] As many Western social media platforms remain blocked in China, local providers have created similar versions. For example, Tencent's QQ and Weibo are popular blogging and messaging services. QQ is anonymous to an extent as people are identified by number. However, this only maintains anonymity from the general population because one has to formally register in order to use the service and this information would be available to the Chinese government.

People on standard mobile phone contracts or fixed phone lines already had to register in order to obtain a service. However, pre-paid SIM cards were still available without registration. Nevertheless, this was changed on 1

---

867 National People's Congress Standing Committee Decision concerning Strengthening Network Information Protection, adopted on 28 December 2012 at the 30th Committee Meeting of the 11th National People's Congress Standing Committee, <https://chinacopyrightandmedia.wordpress.com/2012/12/28/national-peoples-congress-standing-committee-decision-concerning-strengthening-network-information-protection/> accessed 19 January 2017,I

868 Ibid., II-IV

869 Westin (n 42) 31

870 Sanja Kelly and Sarah Cook, 'New Technologies, Innovative Repression: Growing Threats to Internet Freedom' in Sanja Kelly and Sarah Cook (Eds.) *Freedom on the Net 2011: A Global Assessment of Internet and Digital Media*, (Freedom House, 2011),19

September 2010 when the MIIT required that all people purchasing a SIM card present valid identification in order to register. Although this was aimed at stopping spam and fraud, it also removed the remaining method of anonymous communication in China.[871]

In addition to the above, China put into place a regulation that requires people to use their real names when they sign up for Internet services. Since December 2012, service providers have been required to obtain the real names of subscribers.[872] This, in fact, delivered a hard blow to anonymity on the Internet in China.[873]

Furthermore, access to free Wi-Fi services in China is not anonymous. For example, to gain access to McDonald's Wi-Fi service one first needs to enter one's name, email and China Mobile phone number. A Short Message Service (SMS) message is then sent to the number entered with further instructions. In this way, the ISP will log your personal details and these can be tied in with your mobile number.[874]

In spite of this, in reality, there is little difference between the situation in China and that of the US and UK. For example, McDonald's in the UK now require some personal information before one can use their free Wi-Fi,[875] and, in

---

[871] http://www.chinadaily.com.cn/china/2010-09/01/content_11243699.htm accessed 22/08/11

[872] National People's Congress Standing Committee Decision concerning Strengthening Network Information Protection (n 867) VI

[873] Jyh-An Lee and Ching-Yi Liu, Real-name registration rules and the fading digital anonymity in China, 25 Pac. Rim L. & Pol'y J. 1, 2016, p13

[874] Captured during a test session at a McDonalds in Beijing, summer 2011: Pursuant to Article 23 of "Regulations on Administration of Business Premises for Internet Access Services of the People's Republic of China", network operator is required to collect personal particulars from Internet users, please fill in below and click "Continue" to enjoy the FREE Wi-Fi Service.

[875] See McDonald's Free Wi-Fi FAQ at http://www.mcdonalds.co.uk/ukhome/Restaurants/Free-WiFi/Free-WiFi-FAQs.html accessed 26/3/16 which states that in the UK one needs first to register; the US information does not suggest that registration is

general, one will need to register personal information and credit card details for home broadband.

In this research, it is clear from the evidence and examples shown that China has a sophisticated technological mechanism with which to control the Internet. Although the principal aim of this mechanism is to control information and apply censorship, it invades privacy in doing so. Anonymity is outlawed – people are required to register using their real names in order to use the Internet. However, in recent years, a right of privacy has been found from an unlikely source – the human flesh search which by nature is the antithesis of privacy.

The human flesh search, which originated in China, is massively privacy invasive, becoming a 'striking phenomenon'.[876] Human flesh searches involve groups of people finding out everything they can about a target individual and then making that information public. Chinese web users would perform human flesh searches to identify 'corrupt government officials and individuals engaged in other illegal or unethical activities'[877] and thus, turning surveillance back onto the state.

There is the possibility of action under law against service providers who carry information as a result of a human flesh search. This is because providers must not 'produce, reproduce, publish, or disseminate'[878] information, the

required, see http://www.mcdonalds.com/us/en/services/free_wifi.html accessed 26/3/16

[876] Xue (n 231) 288

[877] Fei Yue Wang and others, A study of the human flesh search engine: crowd-powered expansion of online knowledge, IEEE Computer Society, August 2010, 45-53, p45

[878] Measures for the Management of Internet Information Services Art. 15. The text is available in 43 Chinese Law and Government 5 (Sept-Oct 2010) 30-35, translated by Ted Wang

contents of which 'spread rumours, disturb social order, or undermine social stability'.[879]

On the face of it, this is not actually anything new. Ever since search engines were created and people put their information online it has been possible to use search sites to gather information about an individual. However, this research noted that what was new was the way it became a phenomenon, using groups of people and both online and offline sources.

However, the case of *Wang Fei v Zhang Leyi, Daqi.com and Tianya.cn*[880] would have a significant outcome. Wang had had an affair and on its discovery his wife committed suicide after blogging the facts and her intention. The ensuing human flesh search collected and disclosed Wang's contact information along with that of his family and his alleged mistress. Wang sued Zhang Leyi, a friend of Wang's wife, who had published information about Wang and his affair on a website, along with two other websites which had also published the information – daqi.com and tianya.cn – which also published the information. The Beijing court found Zhang and daqi.com to be liable for causing emotional distress to Wang; tianya.cn had removed the information previously and was not prosecuted.[881]

Previously, the courts in China had always tied any concept of privacy to the right to reputation. In the *Wang Fei* case the court took privacy as a separate issue. In what Ong describes as a 'landmark decision'[882] the court determined that a person's love life is private, and privacy includes those facts that one

---

[879] Measures for the Management of Internet Information Services Art. 15(6). The text is available in 43 Chinese Law and Government 5 (Sept-Oct 2010) 30-35, translated by Ted Wang

[880] Wang Fei v Zhang Leyi, Daqi.com and Tianya.cn, Beijing Chaoyang District Court, No. 10930 (2008) <http://old.chinacourt.org/html/article/200812/18/336418.shtml> accessed 21 March 2016

[881] Anne S Y Cheung, China Internet going wild: Cyber-hunting versus privacy, Comp. L. & Security Rev. 25 (2009) 275-279, 276

[882] Rebecca Ong (n 226) 175

does not wish others to know. Zhang had infringed Wang's right of privacy by publishing his personal information. This is a clear violation of autonomy - as stated by Kupfer (Section 2.2 page 18) autonomy gives us control over what is known about us.

5.6 Conclusion

China is an ancient country with a new legal system which has both embraced and attempted to control the Internet. Yet, the Internet is just one, relatively new method of communications and China attempts to control the whole sphere of communications technologies. Mobile phones do not escape the censor. SMS services can be scanned for keywords and messages blocked; or, in some cases service to that mobile phone terminated. Due to the ease with which mobile phones can be used to organise protests, China has sought to increase its control over such services.[883]

China's surveillance and real name policy leaves little room for Internet privacy, at least from state actors. China is thus presented as the worst case scenario, one which the West is getting ever closer to. The similarities are stark. For instance, China's content filtering and blocking is simply a larger scale version of that which occurs within school networks in the UK. The ability to block offending sites is echoed in the UK where courts can order ISPs to block infringing websites. Finding people that have accessed terrorist websites or that publish terrorist material is, in fact, no different from finding those accessing or disseminating information about Falun Gong.

After examining the situation in detail within the contexts of the US, the UK and China, the research has found that the three are not that different when it comes to the invasion of Internet privacy. One may wonder whether there are any technical solutions and/or measures that can preserve Internet privacy. This becomes the core discussion theme in the next chapter, focusing both on technical measures to maintain Internet privacy and the equal and opposite

---

[883] China Media Bulletin, issue 5 January 13 2011, 'Chinese government expands mobile-phone controls'

technical measures implemented by the intelligence agencies as revealed in the 2013 Snowden revelations.

Chapter 6: Enhancing Internet privacy; expanding Internet surveillance

6.1 Introduction

The previous chapters have investigated Internet privacy, describing how the Internet works and indicating where communications surveillance may be carried out with particular focus on the US, the UK and China in order to advance our understanding of whether privacy has any place left in the Internet in these three culturally and politically different jurisdictions.

In this chapter, the focus is now turned to addressing the question 'what measures can be taken to prevent mass Internet surveillance from destroying Internet privacy?'. Of note, in this chapter the scope of investigation is primarily based on the technical perspective. Also, of note, in the course of the investigation conducted by this research, particular reference is made to the 2013 Snowden revelations. This is because the issues examined here are global in reach as the Internet is truly global in scope and surveillance techniques are not bound by geography.

In this chapter, web access is used as an example of a common Internet application. The reason for choosing this from amongst the plethora of Internet applications is that its use is widespread, not only via browsers on home computers, but also apps on mobile devices. It is important to understand the functioning of the Internet from a technical perspective building on Chapter 2. This is because while the Internet remains largely hidden from view behind the user friendly applications of today, it is necessary to understand exactly what data is transferred both when we use those applications and even when a device is simply turned on. The situation is made worse by the utility of smart devices which may have a number of network-aware features communicating all the time, potentially including the user's identification or other identifying

information.[884] Even where information is encrypted, these data transfers will still leave a metadata trail.

The outlines of this chapter are first to examine web browsing from a technical perspective in order to understand how and where privacy can be invaded. Such access may be for any number of reasons including access to static web pages, social media websites, news sites, or e-mail via a webmail service. Access may be passive, in that one reads information, or interactive such as posting a message on a social media site or composing e-mails via webmail. In each case, there will be a metadata trail left by the access, and as will be shown this may be in multiple jurisdictions. Then a set of technical privacy protection mechanisms are explained and presented. Finally, evidence of mass Internet surveillance are presented and discussed, leading to a set of useful insights to conclude the chapter.

6.2 Mechanics of website access

When a browser accesses a web page, several things occur during that access. For the purpose of this discussion a website address[885] can be considered to have two component parts, namely the address of the host web server holding the required web page, and the path to that web page if required. For example, the URL http://www.leeds.ac.uk/info/5000/about illustrates these two component parts. As defined above the host is www.leeds.ac.uk and the path is /info/5000/about. However, the latter component may be omitted if the page required is the websites index page, for example http://www.leeds.ac.uk/ will return the home page for that website.

---

[884] The iPhone, for example makes a connection to Apple's 'Find my iPhone' service as well as cloud and e-mail providers. In an experiment, it was found that an iPhone 4S made 27 separate DNS requests between the time it was switched on and the time it became available for use. All were to Apple services.

[885] Web addresses are termed Uniform Resource Identifiers, see Tim Berners-Lee, R Fielding and L Masinter, Network Working Group RFC3986 Uniform Resource Identifier (URI): Generic Syntax, January 2005, s.3 <https://tools.ietf.org/html/rfc3986> accessed 11 June 2016

The URL is the visual aspect of this process and what the user sees. It gives little clue as to the underlying technology. Once typed into the browser's address bar or clicked on if it is a link in some other page, the user's device will first request the IP address of the host, www.leeds.ac.uk (in the above example), from the DNS. Once it has the IP address, 129.11.26.33 in the case of www.leeds.ac.uk it then makes a connection to the remote host. By convention, normal web page access uses port 80, whereas encrypted access uses port 443. Typically, these are selected automatically by default with http:// accessing port 80 and https:// accessing port 443.

In order to access a required web page (such as /info/5000/about in the above example), the browser now sends commands and information to the remote host to request it. The host will then return the requested page. It is important to realise that the remote host may serve a number of websites. Among the information passed to the host server is the name of the host that is actually required. The web server in the above example hosts numerous websites including www.leeds.ac.uk, medhealth.leeds.ac.uk, ses.leeds.ac.uk, and purchasing.leeds.ac.uk. In order to select the relevant website the server needs the name of the host requested and, referring to Chapter 2 this is not a part of the information needed to route packets across the Internet. The web server will unpack the data in its entirety and access the host name which is in the deepest part of the packets along with the actual content of the communication.[886]

Now that the remote host has received the information it needs, it sends the web page to the user's browser. Once it has completed sending the page, the server will typically log the transaction in a log file. Information recorded in the log includes the user's IP address, the address of the web page or resource requested, and may include the previous URL visited and information about the user's browser. Once the web page has been received, there are still more steps before the page is displayed in the browser. It is important to understand

---

[886] There is an exception to this where the data is encrypted. In such a case the web server needs advanced notification of the host name and this is examined in Chapter 6.

that a modern web page will rarely be simple text, but will also include graphics and code which forms the overall design in which to display that text. It may also contain analytics and advertising code, all of which can refer to a different web server anywhere on the Internet. The user's IP address and potentially their browser information (as shown above) can be recorded by each web server serving each individual part of the website because the browser must connect to each server in order to download the requested material.

What at first may seem a simple web page request may actually result in connections being made to many web servers as illustrated in Table 6.1[887]

Table 6.1: IP addresses accessed by a browser while accessing www.asda.com

URL	IP address	Area
http://www.asda.com	95.101.128.147	UK
http://www.asda.co.uk	161.170.248.158	US
http://b.wal.co	184.30.96.35	UK
http://www.googleadservices.com	216.58.213.98	US
http://js.dmtry.com	2001:4860:4802:32::1b	US
https://fonts.googleapis.com	2a00:1450:4009:804::200a	Eire
https://googleads.g.doubleclick.net	2a00:1450:4009:805::2002	Eire
http://www.googletagmanager.com	2a00:1450:4009:804::2008	Eire
http://walmartasda.d2.sc.omtrdc.net	66.235.148.132	US
https://www.google.com	2a00:1450:4009:804::2004	Eire
http://log.dmtry.com	54.88.143.253	US
https://www.google-analytics.com	2a00:1450:4009:804::200e	Eire
https://5832323.fls.doubleclick.net	216.58.214.6	US
https://www.google.co.uk	2a00:1450:4009:804::2003	Eire
https://stats.g.doubleclick.net	74.125.206.154	US
http://static.hotjar.com	108.161.188.192	US
https://www.facebook.com	31.13.90.36	UK
http://cm.g.doubleclick.net	216.58.213.98	US
https://beacon.asda.com	161.170.236.122	US
https://script.hotjar.com	94.31.29.64	UK
http://dev.visualwebsiteoptimizer.com	5.10.110.36	UK

[887] Browsing to http://www.asda.com/ using Firefox with the IPvFox plugin which reveals what connections the browser made. Location and ISP information discovered using iplocation.net. 2/Dec/2016

Like many other websites, the Asda website is rich in design elements and functionality and this is why there are so many requests for what is essentially just the home page of their website. However, this simple example adequately illustrates the complexities of a modern website and also shows how one's personal information, or at least IP addresses can be recorded in other jurisdictions. Most importantly, this research shows how little control over or knowledge of this the user has. Personal information, via metadata, is left (or retained) at each step when people access websites. An IP address has the potential to be classed as personal information and a threat to anonymity. As stated by Westin (Section 2.2 page 20) anonymity enables one to be free from 'identification and surveillance'[888] and yet, even at this most basic level one can already see how this is put at risk.

6.2.1 Privacy issues caused by browser pre-fetching

One can see from the above given example that when a web page is accessed a data trail may be left. Web server logs may contain a record of the visits made by your browser, and web servers not seemingly involved with the delivery of that web page may also record similar details because they have served certain parts or functions of the page.

There is one other mechanism of note here – pre-fetching. Here, the web browser will examine the page the user has just accessed and will make access to associated content in the background to save time in case the user wishes to access this. For example, a news website is accessed and the browser then accesses the five top stories in case the user wishes to access one of these. This mechanism exists in order to give an apparent speed-up of access. From the user's perspective, the page loads quickly because the browser has already downloaded it. However, there is an implication. The pages which have been pre-fetched may never be accessed by the user, but have been accessed by the user's browser through no action on their part. Each access will have left the same metadata trail as outlined above. As illustrated in this research, this is another example of a hidden data transfer

---

[888] Westin (n 42) 31

which could conceivably make access to information which may put the user under suspicion.

6.2.2 Cookies and the implications for privacy

There is one other common factor which can be privacy invasive. Cookies are text files which can be placed on and read from the user's device. These are used for a wide variety of purposes, and can be set in such a way that only a specific web server can access them, or so any number of servers in a specific domain can gain access. For example, a cookie may be set such that only the web server supporting www.leeds.ac.uk can access, or that access can be made from any server within leeds.ac.uk. The use of cookies is regulated at the EU level and was covered in Chapter 2. Cookies are more invasive than an IP address. As discussed in Chapter 2 an IP address does not identify a specific system but a cookie is stored on the system itself potentially opening up the possibility of tracking a specific system as it visits different websites which can read the same cookie.

Cookies may be used to control functions such as shopping carts, or may be used to control advertising, to name just two such uses. However, if one were able to trick the user's browser into sending cookies, an adversary could potentially learn personal information about the user. For example, webmail sites will typically store the user's details in a cookie to speed up access controls. Snowden revealed just such a use which will be examined in Section 6.6.3 below.

6.2.3 Browser summary

As aforementioned, browsing the web can result in one's IP address being logged by multiple servers in multiple jurisdictions and this is rarely evident to the user. If one is interacting with a website it is reasonable to assume that any data one sends will be recorded by that site, but exactly where else it may be recorded is often not obvious. For example, one may interact with a UK website but actually send personal information to a website in the US as a result. Accesses to a given website may result in accesses to many other websites behind the scenes and unknown to the user. Combine this with the

fact that mobile devices make such access all the time, certain apps are loaded regardless of whether or not we are using them and one can see how privacy may be put at risk. The metadata we leave as a result may be left in multiple jurisdictions and often on a different continent to the website we are accessing. As stated by Wacks (Section 2.2 page 18) this removes our freedom to choose to be private. Despite all these, there is another factor controlling where our Internet data may be sent, and this is presented next.

6.3 Internet routing

The previous section showed how the common task of using a web browser to access a website can lead our IP addresses, as a minimum being recorded in multiple jurisdictions. However, the way that data is routed across the Internet can also lead to unexpected loss of informational privacy. From a user's perspective the Internet transfers data from one edge to the other and the user is unaware of the complexities within. While a user using the Internet to communicate with a web server may see it as a straight line path, peering arrangements and intervening geography shape the network path actually being used. In order to illustrate aspects of Internet routing, Table 6.2 is used to show the path that data took between Brazil and South Africa, both points in the Southern Hemisphere:[889]

Table 6.2: A simplified traceroute from Brazil to South Africa

1	gw-pinger.unesp.br	200.145.255.42	Sao Paulo, Brazil
2	miami15.mia.seabone.net	195.22.199.209	Miami, US
3	ashburn2.ash.seabone.net	195.22.199.185	Ashburn, US
4	AEQ-Ashburn.as6453.net	216.6.87.202	Ashburn, US
5	NJY-Newark.as6453.net	216.6.87.242	Newark, US
6	SV8-Highbridge.as6453.net	80.231.138.17	Highbridge, UK
7	PV9-Lisbon.as6453.net	80.231.158.6	Lisbon, Portugal
8	KLT-Cape-Town.as6453.net	80.231.159.62	Cape Town, South Africa
9	ns2.gcis.gov.za	164.151.129.19	Cape Town, South Africa

[889] http://ping.unesp.br/cgi-bin/traceroute.pl?target=164.151.129.19 accessed 02/12/16

In Table 6.2, steps 2 to 3 involve the Seabone IP backbone operated by Telecom Italia Sparkle.[890] There are several potential oceanic cable routes between Brazil and the US, but it was not possible to determine the exact one.[891] At step 4, the route passes from the Seabone IP backbone to the network operated by Tata communications.[892] Between steps 5 and 6, the route traverses the TGN-Atlantic cable[893] while between steps 6 to 8, the West Africa Cable System (WACS) is used.[894]

From an Internet privacy perspective although a user in Brazil communicating with another user in South Africa may view the Internet as a direct line between the continents, their data actually goes via both the US and the UK, putting it at risk of interception as revealed in the 2013 Snowden revelations. Six Cable Landing Stations (CLSs) are involved, two per each oceanic cable, each of which provides a useful bulk Internet tapping point. Of particular note, the Internet hub at Ashburn, US is claimed to carry 70% of the world's Internet traffic,[895] an ideal location for an NSA tap.

---

[890] See <http://whois.domaintools.com/seabone.net> accessed 22 January 2017

[891] See for example Monet <http://www.submarinecablemap.com/#/submarine-cable/monet and South America 1 http://www.submarinecablemap.com/#/submarine-cable/south-america-1-sam-1> accessed 2 December 2016

[892] See <http://whois.domaintools.com/216.6.87.202> accessed 22 January 2017

[893] See <http://www.submarinecablemap.com/#/submarine-cable/tata-tgn-atlantic> accessed 2 December 2016

[894] See <http://www.submarinecablemap.com/#/submarine-cable/west-africa-cable-system-wacs> accessed 2 December 2016

[895] Sean Buckley, 'Windstream establishes 100G express route in red-hot Ashburn, Va. Market via NJFX', (*FierceTelecom*, 19 January 2016) <http://www.fiercetelecom.com/telecom/windstream-establishes-100g-express-route-red-hot-ashburn-va-market-via-njfx> accessed 2 December 2016

Covert methods or technical failures can also modify the path taken. In February 2008, the Pakistan government instructed Pakistani ISPs to block access to YouTube. Pakistan Telecom changed its routing tables to attempt to route YouTube calls to a web page stating that YouTube had been blocked. Unfortunately, in so doing, it advertised the routing change to its upstream providers which advertised the route change further, resulting in the Internet at large then routing all YouTube connections to Pakistan for a short while.[896] In March 2011, a routing error in AT&Ts network routed Facebook connections via China and Korea.[897] In the case of the action by Pakistan Telecom, YouTube became unavailable. However, in the AT&T case, users would be unaware that their data was being routed via China and Korea as Facebook was still accessible. The AT&T case indicates how a government could covertly change Internet routing to its advantage, forcing it to pass across its tapping point.[898]

From the above sections one can see how personal information may be left in foreign jurisdictions that are not apparently associated with the web service one accesses. At a minimum the IP address of a person's device will be recordable as connections are made to the various web servers associated with a web page. Additionally, the actual communications path taken may be unexpected, again presenting the risk of one's personal information being recorded by, for example the US and the UK even when the services one accesses are in a different continent.

---

[896] See www.wired.com/threatlevel/2008/02/pakistans-accid/ accessed 27/Oct/13

[897] See www.blyon.com/hey-att-customers-your-facebook-data-went-to-china-and-korea-this-morning/ accessed 27/Oct/13

[898] Kevin Butler and others, 'A Survey of BGP Security Issues and Solutions', 98 Proc. IEEE 1, January 2010, p100-101

6.4 Deep Packet Inspection

The previous sections explained and illustrated potential risks for privacy when using common Internet applications. Evidently, there are a number of places where an adversary may acquire data in transit across the Internet.

Clearly, if an adversary can access all the data packets forming a communication they will be able to access the content which may contain personal information. The content of a communication is generally protected in the laws in the US and the UK as covered in Chapters 3 and 4, respectively. It is not so protected in China, and it is indeed clearly accessed by filtering software and the army of censors as was discussed in Chapter 5.

There is another component part which itself can be privacy invasive. Metadata indicates the facts of a communication, for example where it came from and where it is going. This was already discussed and presented in Chapter 2. Accessing this data is not as straightforward as a telephone tap or a pen register. Most of the metadata of interest is contained deep within the data packets and it is necessary to understand the essential technique necessary to access it. In order to understand how data can be extracted from packets of information passing across the Internet it is necessary to examine the communications protocol and the structure of packets more closely.

As was described in Chapter 2 packets of data are routed across the Internet depending on the addressing information they contain. The actual content of a communication may be spread across many data packets or may be held in a single packet, depending on the size of the data. This content is of no interest to the systems responsible for delivering it: routers need access to IP addresses and so they access the Internet layer (OSI layer 3). The deeper we look into the packet, the more information we can find. Shallow Packet Inspection (SPI) can be used to access the Transport layer (OSI layer 4) where it then has access to TCP ports. This may be used for resource management; an example being to route web traffic to one server and video traffic to another, or to throttle the speeds of some types of traffic to permit greater bandwidth for others. However, the technique known as Deep Packet Inspection (DPI) decodes the entire packet and thus, can gain access to the

payload data. Data in this case contains a mixture of content and metadata. For example, the headers of an email and the requests for a web page exist at the Application layer (OSI layer 7) along with any content.

Figure 6.1: simplified data packets[899]

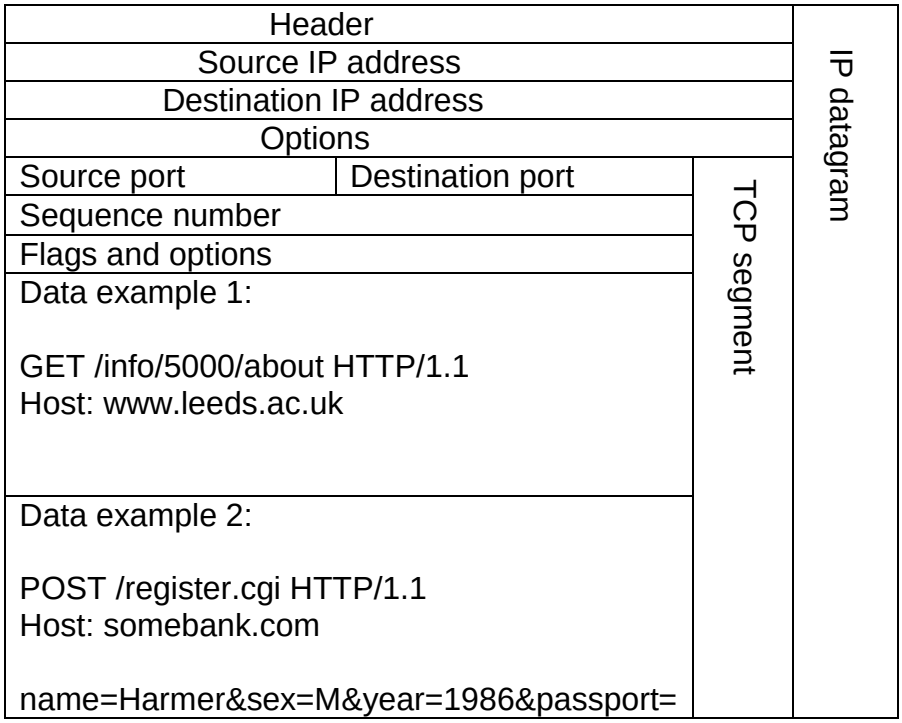


Figure 6.1 shows two simplified examples of data contained in a packet. The first example (Data example 1) is a request for a web page while the second example (Data example 2) is a request to send data to an application on the web server. This illustrates the complexity of extracting metadata required under the US and UK surveillance laws. The data field contains a mixture of metadata and content. In Data example 1, this is the sequence that would be sent as a browser request for http://www.leeds.ac.uk/info/5000/about. The GET command informs the web server of the file required and will be defined as content. The following line indicates the host name (www.leeds.ac.uk in the above example) and is defined as metadata because it is here only that the

---

899 For a description of the formats and fields, refer generally to RFC791 <https://tools.ietf.org/html/rfc791> accessed 18 December 2016), and RFC793 <https://tools.ietf.org/html/rfc793> accessed 18 December 2016, and their updates.

server part of the URL appears in the data. As was described earlier, the IP address rarely yields the web server name. Data example 2 shows data being sent to a remote application. Again, the first line is content and the second is metadata. The content data appears after these lines. As all parts of the packet are accessible at this level, care must be taken to separate metadata from content.

The UK's plans to record ICRs was already discussed in Chapter 4. DPI is a requirement in order to make ICRs feasible because at the very least, ICRs require the recording of host names. Wherever DPI is in place, one simply needs to extract the HTTP host header as is shown in Figure 6.1.[900]

As was discussed in the above sections our activities on the Internet can leave our personal information or potential identifying information in any number of jurisdictions, thus posing issues for our Internet privacy. The structure of the Internet is such that surveillance can easily be carried out at a number of points. Additionally, it is never clear to the user exactly where their data will go when it traverses the Internet. Internet communications consist broadly of two components – the content of the communication, and the metadata associated with the transmission of that content – and whether these can be protected is discussed next.

6.5 Technical methods of improving Internet privacy

In order to maintain Internet privacy two component parts of a communication must be protected. The content of a communication is the easiest of the two because encryption can be used. This is described below. However, as will be explained the metadata, which consists of information including the fact that the communication took place as well as who the sender and recipient are is more difficult to protect.

---

[900] Science and Technology Committee (Commons), Investigatory Powers Bill: technology issues <http://www.publications.parliament.uk/pa/cm201516/cmselect/cmsctech/573/57305.htm>, 26

6.5.1 Protecting the content – encryption

Encryption is the process of converting a message into a cryptogram (or ciphertext),[901] and cryptography is the set of techniques which enable this encryption. A key is needed to unscramble the message to produce the original.[902] There are three common cryptographic techniques employed on the Internet, namely digital certificates, symmetric key cryptography, and public key cryptography. Depending on the communications mechanism used, these three cryptographic techniques may be used sequentially, and this is depicted below.

Symmetric key cryptography is a symmetrical system with a single key being used to both encrypt and decrypt the information to be passed between parties. Both the sender and receiver need the same key. The principal issue with symmetric key encryption is how the communicating parties obtain the key. For instance, if Bob wants to send encrypted information to Alice, he has to first send the key to Alice. If Eve obtains this key in transit, Eve can decrypt any information sent between Bob and Alice.

Unlike symmetric key cryptography, public key cryptography uses two keys - one public and freely distributable, and one private, the security of which is critical. A message encrypted with a user's public key can only be decrypted by their private key and vice versa. Here, when Bob wants to send an encrypted message to Alice, he obtains her public key and uses this to encrypt the message. Alice then uses her private key to decrypt the message, and vice versa. Even if Eve obtains the public, keys she cannot decode any of the messages as she does not have either private key.

Despite this, there are two issues with public key cryptography. The first issue is that it is computationally expensive and therefore, it is only suitable for short exchanges. In order to exchange encrypted information more efficiently

---

[901] Don J Torrieri, *Principles of secure communications systems (2nd edn.)* (Artech House, Boston, 1992), p463

[902] Whitfield Diffie and Susan Landau (n 336) p13

symmetric key encryption is used, with public key encryption used first to exchange the symmetric key in a secure fashion. The second issue with public key cryptography is 'how does Alice know that Bob really is Bob?'. Eve could just as easily publish a public key in Bob's name and sent this to Alice; therefore, Alice could unknowingly be communicating with Eve. It is here where digital certificates play a role. A digital certificate has some form of proof attached to it, typically obtained when the certificate is purchased from a Certificate Authority (CA). For example, a CA may request copies of passports and proof of address, though procedures can be weak as illustrated by the fact that two researchers were able to trick Comodo's automated checking system into producing a certificate for a server which they had no relationship with.[903]

Digital certificates contain the user's or server's public key, an expiry date, and other validation information. The overarching standards and processes that permit the creation of certificates forms a Public Key Infrastructure (PKI). Public key cryptography was seen as a threat both by GCHQ and the NSA who 'doggedly fought'[904] against it.[905] Once a message has been encrypted, it can only be decrypted in one of two ways: using the relevant key; or by a brute force attack. The latter mechanism is described by Parker Voors as

---

[903] Shaun Nichols, 'Como-D'oh! Infosec duo exploits OCR flaw to nab a website's HTTPS cert', (*The Register*, 21 October 2016) <http://www.theregister.co.uk/2016/10/21/comodoh_researchers_exploit_image_recognition_bug_to_steal_certs/> accessed 30 October 2016

[904] Richard J Aldrich, *GCHQ: the uncensored story of Britain's most secret intelligence agency* (Harper Press, London, 2010), p492

[905] At one stage the US government was so concerned at the evolution of encryption technologies outside of the NSA's control that it classified them as munitions, meaning strict export controls could be applied. See David Baron and Victoria Chang, Sophis Networks and encryption export controls (A), Graduate School of Business, Stanford University, case no. Sp-34(a), 2000, p8

someone ‘holding a key ring with millions of keys, trying each key in the lock’[906] until a match is found.

Proposals such as key escrow, where all or part of a key would be lodged with a third party, or key recovery, where the encryption system itself effectively had a back door were planned, but the availability of strong encryption from European countries made this unworkable.[907] However, RIPA did incorporate a section to deal with the issue of encryption. Part III of the Act came into force on 1 October 2007[908] and dealt with this subject. Essentially, in order for the intelligence and law enforcement agencies to have any hope to gain access to the contents of an encrypted communication, they need to obtain the encryption keys[909] by issuing a notice under RIPA s.49.[910] The penalties involved raise an interesting issue: for example, when faced with a sentence of 10 years to life for possession of child abuse images a person may choose to refuse to decrypt these for the lesser sentence of up to two years.[911] One may wonder how effective s.49 will be against the criminal underworld or, indeed, a hardened terrorist. This has already been noted by the courts, for example, in *Harlan Laboratories UK Ltd & Anor v Stop Huntingdon Animal*

---

[906] Matthew Parker Voors, ‘Encryption regulation in the wake of September 11, 2001: must we protect national security at the expense of the economy?’, 55 Fed. Comm. L.J. 331 2002-2003, p336

[907] Aldrich (n 904) 492

[908] SI 2007/2196

[909] Although it is technically possible to break many forms of encryption by brute force means, the computing power and time required can be enormous. However, this is further discussed in Chapter 6.

[910] A principle argument against RIPA s.49 was that being forced to hand over an encryption key could lead self-incrimination and would thus breach ECHR Art. 6. However, this was clarified in R v S and A [2008] EWCA Crim 2177 in which it was determined that an encryption key merely makes readable evidence that is already in the lawful possession of the police and the key by itself is no different to the key to a locked drawer.

[911] HC Deb 06 March 2000 vol 345 cc767-835 at col.812; See RIPA (n 689) s.53.

Cruelty ("SHAC") & Anor[912] that one of the defendants willingness to be prosecuted under RIPA s.53 indicated the extent to which he desired to keep his material out of police hands.[913] Even as modified by s.15 of the Terrorism Act 2006 the maximum term of imprisonment under RIPA s.53 is five years in national security cases. This section of RIPA seems more focused on the 'average citizen' who, faced with the threat of legal action under the Act is most likely to hand over the keys with little regard to their privacy.

Although there are weaknesses in the CA model and PKI itself which will be discussed in Section 6.6.2 below encryption is a proven mechanism for protecting the *content* of communications, but this leaves the issue of the metadata. This is discussed next.

6.5.2 The problem of metadata

Encryption is a viable means to protect the content of a communication provided the method of encryption itself remains secure. The increasing use of End-to-End Encryption (E2EE), in particular in apps, means encryption is always enabled and that the supplier has no access to the encryption keys. Therefore, the provider cannot be compelled to assist with decryption. Where encryption is used to access web resources, only the source and destination IP addresses and ports, and potentially the web server's host name, remain accessible as metadata. The metadata trail between communicating users can also be broken by passing communications via a central server. In such a case communications metadata will only show Bob communicating with some central server, and later Alice communicating with the same server but not with each other.[914] WhatsApp[915] offers voice, video and messaging

---

[912] EWHC 3408 (QB) (7/12/12)

[913] EWHC 3408 (QB) (7/12/12) at 43

[914] If the server itself or its Internet connections were being surveilled it may be possible to match Bob and Alice if the timing of the communications suggested a link. However, this may be impractical on a busy server with numerous simultaneous connections.

[915] See https://www.whatsapp.com accessed 03/01/17

between people and uses E2EE by default. For messaging WhatsApp routes these through central servers.

However, for more general Internet communications such as accessing websites connections are made between the user's browser and the target web server and the metadata trail is left accessible. Only the data part of the TCP segment can be encrypted as otherwise communications would not be possible – for example, the IP addresses and TCP ports must still be available. Although the HTTP headers are a part of the encrypted content there is a further weakness in the requirement that the name of the host being connected to be sent in clear text by Server Name Indication (SNI).[916] This is done to enable a web server to select the relevant digital certificate to be used to enable encryption, but it means that this important piece of metadata is still available regardless of encryption. In other words, even when encryption is used, the host name is still available using DPI.

In order to protect one's metadata as well as content, there would need to be a way to encrypt or otherwise, hide that metadata. One method is to use a VPN where the only metadata trail from one's device is to the VPN server. Communications between the client and the VPN server are encrypted. The VPN server is then used to make onward connections and communications. For scenarios such as ICRs, it means the ICR would only ever record the connection between the client and the VPN server, not the target website.

VPNs are a practical way to maintain one's Internet privacy, but an adversary with sufficient resources and metadata could still potentially determine the end-to-end path. For example, if a VPN was supporting only one client one may assume that any onward connection from the VPN is done as a result of a request from that client. If the VPN were supporting a number of simultaneous clients this becomes problematic. However, there is a system which provides anonymity by using a mixture of encryption and routing via

---

[916] Donald Eastlake, 'Transport Layer Security (TLS) Extensions: Extension Definitions', RFC6066 <https://tools.ietf.org/html/rfc6066> accessed 19 November 2016

different systems which are widely dispersed, and which also encrypts the actual metadata. This is described next.

6.5.2.1 Onion routing – Tor

The issue of metadata can be solved by the use of onion routing. In conventional routing, the source and destination IP addresses are held in each data packet and thus, enabling the communication to be routed to its destination, but also allowing the data to be traced. Onion routing breaks this by the use of both encryption and multiple varying paths through the Internet. Tor[917] is a decentralised mesh of computers spread throughout the world, with accessible entry and exit points, and a random path between interconnecting nodes.

The concept of onion routing, also known as telescopic encryption,[918] was originally developed by the US Navy Research Laboratory primarily to protect government communications.[919] By using the onion routing technique, Tor enables people to 'improve their privacy and security'[920] while using the Internet. The 'onion' description refers to the fact that Tor encrypts the data once per each node in the chain. By default, a three node circuit is decided by the client browser and the encryption keys for each node acquired. The data and the required routing metadata is then encrypted by each set of keys, starting with the last node and working backwards. Finally, the encrypted bundle of data is sent to the first node. The first node decrypts the first layer of the data to determine where next to send it. This process happens sequentially until the data is sent to its destination by the final node. In this way, each node only knows where the data came from and where to send it

---

[917] Roger Dingledine, Nick Mathewson and Paul Syverson, Tor: the second-generation onion router, Proc. Of the 13th Usenix security symposium, August 2004, 303-320, p303

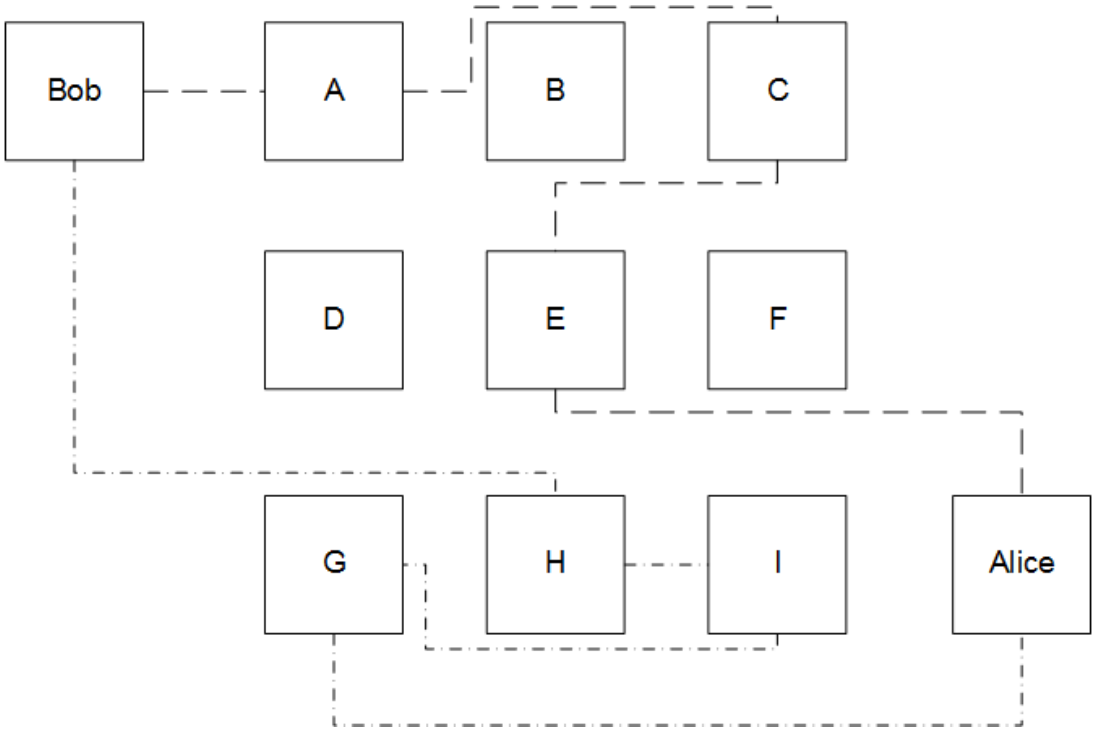
[918] Cormac Callanan, and others, Leaping over the Firewall: a review of censorship circumvention tools, Freedom House, p41

[919] See http://www.onion-router.org/History.html accessed 07/11/12

[920] Ibid.

next; no node knows the entire circuit. Only the first node knows where the client is and it is only the last node which knows the actual destination of the communication. Only the last node has access to the communication itself and if this is encrypted at source, then it remains secure. The communication entering the Tor network is already encrypted, so the first node itself cannot access the content.[921]

Figure 6.2: Tor routing



Consider Figure 6.2. Bob is communicating with Alice. At first, the connection (denoted by the dashed line) goes from Bob to nodes A, C and E, and then to Alice. Later, the connection changes to nodes H, I and G (denoted by the dot and dash line). Later on during their conversation it will change again. For the sake of argument, we will assume that nodes A, D and G are in the US, nodes

---

[921] Damon McCoy and others, 'Shining light in dark places: understanding the Tor network', in Nikita Borisov and Ian Goldberg, (eds.) *Privacy enhancing technologies, Proc. 8th international symposium, PETS 2008, Leuven, Belgium, July 2008* (Springer, Berlin, 2008), 63; see also Joshua A Altman, 'A Schrodinger's onion approach to the problem of secure Internet communications', 7 Wash. U. Global Stud. L. Rev. 103 2008, 112

B, E and H are in the UK, and nodes C, F and I are in Russia. In this scenario, nodes A and H are entry nodes, E and G are exit nodes, and C and I are intermediate nodes. These intermediate nodes are only aware that data is coming from and going to other nodes, but cannot see any information which relates to either Bob or Alice or their IP addresses. The entry nodes see Bob, but have no other information and are unaware of Alice; and, in the same way, the exit nodes know Alice but not Bob. Even if one had access to the metadata from each node as shown in Figure 6.2, if those nodes are busy and thus sending and receiving a lot of traffic it would be extremely difficult to identify the actual user.[922]

Tor is even more secure where two users are communicating wholly within it. For example, the TorChat Instant Messenger uses a hidden service as intermediary between Tor-connected users. As the encryption of any communication sent via Tor is encrypted before it is sent to the entry node, all communications remain encrypted throughout.

6.5.2.2 Disadvantages of using Tor

Websites are often rich in content and functionality. As was discussed in Section 6.2 access to one web page can result in access being made to many other resources across the Internet. While images will be accessed over Tor, some scripts may make direct access, bypassing Tor. The Tor Browser Bundle has options to block scripts and also to attempt https access to websites. File downloads can also bypass Tor. Blocking scripts may result in a lack of functionality on websites and this, along with latency caused by the rate at which data passes through the Tor network can dissuade users from

[922] When observed (07/11/12) there were 2,968 Tor relays online. The exit node, and thus apparent IP address (via the Tor checker) changed after approximately 5 minutes, moving from a node in the US to one in Sweden; then after approx 10 minutes it changed again, this time to a node in Russia.

using it. The average user may not be willing to 'trade their connection speed for the added security and privacy'[923] offered by Tor.

Another significant fact for this research is that China is able to block access to Tor entry points, thus making it difficult for users there to access Tor.[924] The most common method employed to block Tor is to block access to its directory servers, the IP addresses of which are published. To counter this, the developers of Tor have established a series of systems called *Tor bridges* which can be used to connect into the Tor network but which are not themselves Tor nodes and are not listed in the directory. The identity of these bridges can be obtained via other means, for example, via a website[925] or by e-mail.[926]

6.5.3 Improving Internet privacy – summary

The above sections have shown the issues surrounding keeping one's information and communications private. In sum, encryption can be used to secure the content and much of the metadata of communications and, where that is all that is required, then it does provide an easy solution. Where the fact that someone is communicating also need to be made private, VPNs can be used. For a greater level of privacy protection, Tor can be used, albeit with a reduction in the rich user experience that the modern web provides. However, despite the methods explained above there are still ways in which

---

[923] C Callanan and others, Leaping over the Firewall: a review of censorship circumvention tools, Freedom House, p42

[924] See in general Philip Winter and Stefan Lindskog, 'How China is blocking Tor', arXiv:1204.0447, 2 April 2012 <https://arxiv.org/abs/1204.0447> accessed 10 January 2017

[925] <https://bridges.torproject.org>

[926] Sending an e-mail from a Gmail or Yahoo! account to bridges@torproject.org with the text *get bridges* in the body will cause a list of bridges to be e-mailed back. It is important to note that, as Google and Yahoo! e-mail accounts can be obtained anonymously, even this step of the process maintains a level of anonymity

intelligence agencies can surveil the Internet and acquire our personal information while it is in transit. These are examined next.

6.6 Intensifying Internet surveillance

The previous section outlined, from technical perspectives, the issues of privacy in an Internet context, and indicated ways to at least attempt to maintain privacy. However, as explained and demonstrated in the previous chapters of this thesis, there are so many ways that data passing across the Internet may be surveilled. For instance, to recapitulate some of the research findings, one can intercept data either close to or at the client (user's) system, at the target, or as it passes across the Internet. One may surveil only the metadata, or the whole content.

Technically speaking, tapping the Internet is very different from tapping a telephone. In the case of a telephone, a tap may consist literally of wires connected to the telephone line as it leaves the customers premises. Any communications sent or received along that line would be tapped. However, tapping the Internet differs from telephone tapping in two ways: first, there may be a vast number of communications between different parties travelling across the tap, depending on where the tap is applied; second, the content of a communication is buried within the protocols carrying that data and must be extracted. Assuming one has access to a tap, one needs to use DPI to extract the information from the data packets.

In fact, mechanisms for acquiring Internet data are readily available. In the US, for instance, the company Amesys offers such a system[927] and also published information relating to massive surveillance, where all data travelling across a link are analysed and archived for later analysis.[928] The

---

[927] Amesys Intelligence Solutions <https://wikileaks.org/spyfiles/document/amesys/95_critical-system-architect/95_critical-system-architect.pdf> accessed 23 January 2017

[928] Amesys, From Lawful to Massive Interception: Aggregation of sources, <https://wikileaks.org/spyfiles/files/0/21_200810-ISS-PRG-AMESYS.pdf>, slide 11

company claimed this could enable '[g]lobal search and surveillance of all internet traffic'.[929] Such tapping was revealed by Mark Klein in 2006. Klein claimed to have knowledge of a secure room - 641A - within the AT&T building in San Francisco where ISPs optical fibres were tapped. The tapped data could be analysed to give access to the entire data stream of all traffic.[930] Included in the various hardware in room 641A was a Narus STA 6400 semantic traffic analyser.[931] This device was able to analyse all traffic presented to it, via the fibre taps. Narus claims its products have been deployed by governments 'around the world to protect their countries and infrastructure'[932] with the capability to surveil whole networks regardless of speed and size. If located on major Internet backbones or CLSs or China's Great Firewall this claim would appear surprisingly easy to achieve.

Hence, based on the above a though provoking question needs to be asked that if an all-encompassing surveillance system were established, can there be any Internet privacy at all? This becomes the focus of discussion in this section, specifically looking at supportive evidence to testify whether Internet surveillance has been intensified to form a global surveillance mechanism.

6.6.1 Mass Internet surveillance

In the summer of 2013, the defence contractor Edward Snowden began leaking to the Press a number of secret documents from the NSA. He fled the US and worked with the Guardian, Washington Post and New York Times who published a series of articles revealing some of these documents.

---

[929] Ibid., slide 12

[930] See <https://www.eff.org/files/filenode/att/presskit/ATT_onepager.pdf> accessed 17 February 2013

[931] Mark Klein, *Wiring up the big brother machine… and fighting it* (Booksurge, South Carolina, 2009), 127

[932] See <archive.is/JKVOG> accessed 7/July/2013. The original page referred to as <www.narus.com/products/intercept.html> no longer exists but had been copied by the above archive facility

The first document to appear in the Press revealed that on 25 April 2013, the FISC had ordered Verizon to produce, on a daily basis, a record of all telephony metadata for calls both within the USA and from the USA to abroad.[933] Incoming calls to the US from outside or wholly-external communications were not included. This information was to be passed to the NSA for the duration of the order, which expired on 19 July 2013. The order made it clear that no-one was to reveal the fact that this data collection was being carried out.[934]

The Press releases which followed were to indicate the existence of extensive, mass Internet surveillance programmes operated by both the US and the UK such as PRISM, Upstream and Tempora which are depicted below.

6.6.1.1 PRISM and Upstream: mass Internet surveillance programmes

The mass Internet surveillance programmes PRISM and Upstream were revealed in the 2013 Snowden revelations. PRISM deals with direct acquisition of data from key providers while Upstream focuses on gathering data directly from major Internet links. Both programmes operate under s.702 of the FAA.

Several companies are described as being key providers to the PRISM programme. These include Microsoft, Yahoo, Google, Facebook, PalTalk, YouTube (now owned by Google), Skype (now owned by Microsoft), AOL and Apple. It has been suggested that data is taken directly from the servers of these providers.[935] Facebook quickly issued a statement denying that the NSA had a way to access the data they held, claiming to have ‘never received a

---

[933] US Foreign Intelligence Surveillance Court, Re Application of the Federal Bureau of Investigation for an order requiring the production of tangible things from Verizon Business Network Services, Inc. on behalf of MCI Communication Services, Inc. d/b/a Verizon Business Services <www.theguardian.com/world/interactive/2013/jun/06/verizon-telephone-data-court-order> accessed 20 October 2013, 1

[934] Ibid., 2

[935] http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data accessed 21 September 2013

blanket request or court order from any government agency asking for information or metadata in bulk'.[936] However, Facebook also had a patent granted in May 2011, detailing a system which could in some cases automatically send personal data to a requesting law enforcement agency.[937] Moreover, the essence of an ability to tap into providers in the way suggested in the PRISM slides is covered by CALEA which was described in Chapter 3.

Further evidence suggest that companies were indeed working with the government. For instance, a document released by Snowden dating from 2012 discusses the fact that Microsoft had introduced encryption to some services, cutting off PRISM access. Microsoft worked with the FBI to produce a solution.[938] A further document released by Snowden and dating from 2013 indicated that Microsoft had been working with the FBI in providing access to Skydrive (now Onedrive) and that had become a part of PRISMs standard stored communications collection.[939]

The Snowden revelations resulted in a prompt response from the European Commission. Questions about PRISM were posed in a letter to the US Attorney General on 10 June 2013. This letter highlighted the scope of US legislation, stating that 'direct access of US law enforcement authorities to the

---

[936] See https://www.facebook.com/zuck/posts/10100828955847631 accessed 13/nov/13

[937] US Patent 8438181

[938] Microsoft releases new service, affects FAA702 collection <https://search.edwardsnowden.com/docs/Microsoftreleasesnewserviceaffects FAA702collection2014-05-13nsadocs> accessed 29 May 2016

[939] SSO Highlight - Microsoft Skydrive Now Part of PRISM Standard Stored Communication Collection <https://search.edwardsnowden.com/docs/SSOHIGHLIGHT–MicrosoftSkydriveCollectionNowPartofPRISMStandardStoredCommunicationsCollection2014-05-13nsadocs> accessed 29 May 2016

data of EU citizens on servers of US companies should be excluded unless in clearly defined, exceptional and judicially reviewable situations.'[940]

The existence of the PRISM programme was confirmed in a statement from the Intelligence and Security Committee of Parliament which stated that PRISM was a programme 'through which the US Government obtains intelligence material (such as communications) from'[941] ISPs. President Obama also confirmed the existence of the PRISM and Upstream programmes.[942]

It is found by this research, from a privacy perspective, these mass Internet surveillance programmes offer no protections to non-US persons as the Fourth Amendment only applies to US persons.[943] With a considerable percentage of global Internet traffic passing across the US, these surveillance programmes have the capability of accessing personal information not only within a particular nation state, but also on a global scale. As Wacks states (Section 2.2 page 18) this removes our freedom to be private.

6.6.1.2 Tempora: GCHQs mass Internet surveillance programme

An article published by the Guardian indicated that GCHQ had secretly gained access to submarine cables under its Mastering The Internet programme.[944]

---

[940] Viviane Reding, Letter to the US Attorney General from Viviane Reding, Vice-president of the European Commission, 10 June 2013, Ref. Ares(2013)193546

[941] Intelligence and Security Committee of Parliament, 'Statement on GCHQ's Alleged Interception of Communications under the US PRISM Programme' <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/225459/ISC-Statement-on-GCHQ.pdf> accessed 20 July 2013

[942] 'Barack Obama defends US surveillance tactics' (*BBC*, 8 June 2013) <http://www.bbc.co.uk/news/world-us-canada-22820711> accessed 10 July 2016

[943] 50 USC S1801(i)

[944] Ewen MacAskill and others, 'GCHQ taps fibre-optic cables for secret access to world's communications', (*The Guardian*, 21/June/2013)

Submarine cables provide an ideal tapping point for major worldwide communications. As was outlined in Chapter 2, these cables form pinch points in the global Internet, and much inter-regional and all intercontinental Internet traffic will flow through them.

In fact, tapping undersea cables is not new. During the Cold War, the US tapped Russian submarine telephone cables in the seabed in an operation known as Ivy Bells.[945] However, these cables were electrical, not fibre optic and could be tapped by induction. Modern fibre optic cables are a very different technology. These cables come ashore at CLSs which contain apparatus to combine Internet data from all ISPs involved in the cable operation into several light wavelengths which are then sent down the fibre to the remote CLS, and vice versa. Each wavelength typically carries data at a rate of 10 gigabits per second.[946] It would be impractical to tap a fibre-optic cable on the seabed due to the following issues and constraints: (a) these cables run along the ocean floor and would need to be lifted on-board a ship in order to be tapped; (b) the cables also power repeaters located at points along the cable – this is typically between 5,000 and 10,000 volts; (c) CLSs continually monitor the state of the cable and a tap may raise an alarm; (d) if a cable were tapped at a distance from the coast one needs to install a similar cable and associated CLS in order to get the data back to shore. Hence, it is far more practical to compel CLS operators to install taps in their equipment.[947] Tapped data could then be retrieved, via dedicated cables or microwave links. It is important to note that, unless the tapped data can be processed at the

---

<http://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa> accessed 2 May 2016

[945] Grant Hodgson, 'Breaking Encryption and Gathering Data: International Law Applications', 20 J. Tech. L. & Pol'y 39, 2015, 40

[946] As at 2016. Experiments are progressing to move to 40Gbps and beyond.

[947] See for example the Glimmerglass documentation that specifically discusses tapping single wavelengths in optical fibres to permit monitoring and interception http://www.glimmerglass.com/default/assets/File/Documents/app_notes/App%20Notes%20-%20Lawful%20Interception.pdf accessed 25/04/16.

tapping point all of the data flowing across the tapped link must be transported to a remote facility for analysis.

Described as a buffer, Tempora keeps all data acquired for 3 days and the metadata components for 30 days. As of May 2012, GCHQ had access to 46 individual 10Gbps links.[948] Tempora operates under RIPA s.8(4) which permits the interception of external communications without a warrant.[949]

Taken together, PRISM, Upstream and Tempora present a major risk to informational privacy. Referring to Sections 6.2 and 6.3 it is clear that we run the risk of our personal information being recorded in multiple jurisdictions when browsing the web. Additionally, it is often not obvious where websites are located and these are often not in the same country as the user. Given the US and UK operate major Internet hubs and have programmes aimed at collecting Internet traffic data one can see how personal information may well be recorded without our knowledge or control. As stated by Kupfer (Section 2.2 page 18) privacy enables us to decide when to share personal information with others and yet, mass Internet surveillance takes away this control and thus our autonomy. Given this knowledge one may conclude that Internet privacy is in fact dead. While one may consider encryption to maintain privacy to some extent, in particular privacy of the content of communications there are further threats which are discussed next.

6.6.2 Man In The Middle (MITM) attacks on encryption

As was discussed in Section 6.5.1 encryption can secure the content of a communication in transit. However, there are weaknesses in the mechanism which enables encryption to take place. As part of the process which establishes encrypted communications between a web browser and website, the website's digital certificate will be checked by the browser. If anything is incorrect, the browser will issue a warning. Despite this, there are two issues

---

[948] See Tempora in https://edwardsnowden.com/wp-content/uploads/2014/07/tempora.pdf accessed 2 May 2016

[949] *Big Brother Watch and others v United Kingdom*, App. No. 58170/13, 33

with this process which can be exploited by an attacker. First, if there is a problem with the digital certificate sent by the web server it is up to the user whether or not to ignore the warning that the browser will issue. A study in 2013 concluded that although browser warnings can be effective, almost 25% of users ignored malware and phishing warnings and 33% ignored certificate warnings in Firefox, with over 70% of Chrome users ignoring certificate warnings.[950] Second, acceptance of the digital certificate is automatic unless the browser detects a problem. Both of these issues can be exploited in an attack.

A MITM attack can be carried out where a user's browser is sent to a different website than the one requested. One possible method is DNS poisoning. When a user enters a URL into a web browser, this causes a DNS lookup to determine the IP address to use. If the DNS return was altered, the browser can be made to target a different, rogue web server. Another and more direct approach is to simply force information to pass across a suitable tap as shown in Section 6.3. The user will be communicating with the rogue server directly.

As found in this research, this is where the key weaknesses are. When the rogue web server sends its digital certificate, if any part of it is invalid, the browser will issue a warning. If the user ignores this, then communications will commence with the user wrongly assuming they are connected to the web server they originally wanted to access. If, on the other hand, the certificate appears valid, no challenge will be made and the user will be completely unaware they are communicating with a rogue server. For example, on 19 July 2011, the Dutch company DigiNotar detected unauthorised accesses to its systems which had resulted in a number of 'false (but authentic)'[951]

---

[950] Devdatta Akhawe and Adrienne Porter Felt, 'Alice in Warningland: A large-scale field study of browser security warning effectiveness', Proceedings of the 22nd USeNIX Security Symposium, August 14-16 2013, Washington D.C., s.8 <https://www.usenix.org/sites/default/files/sec13-proceedings.epub> accessed 28 October 2013

[951] Justin Hurwitz, 'Trust and online interaction', 161 U. Pa. L. Rev. 1579, p1604

certificates being created. Certificates created included one for Google.[952] The intruder appeared to be in Iran with the intention of using the rogue certificates to spy on users also in Iran.[953]

Of course, even if the above scenario succeeds, unless the user receives what they expected, they may realise something is wrong. For example, Bob accesses Alice's web server but Eve, as MITM, intercepts the connection and routes it to her own server. Unless Bob sees the expected information, he may not be fooled. However, all Eve needs to do is to receive the data request (e.g. the request for a web page) from Bob and retrieve that web page from Alice's web server and send it on to Bob. In such circumstances, Bob will be unaware of any difference. As Eve intercepted the connection from Bob before it reached Alice, Eve can pretend to be Bob and so Alice's web server will also be unaware of the deception too. Eve is truly the MITM. In fact, even an IM conversation could potentially be intercepted in the same way, with Eve intercepting messages from both Bob and Alice but sending her own responses to each.[954] This technique was allegedly used by the NSA to route calls to Google to its own servers.[955]

---

[952] Hans Hoogstraaten and others, 'Black Tulip: report of the investigation into the DigiNotar Certificate Authority breach' (Fox-IT BV, Delft, 2012), p3 <https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/rapporten/2012/08/13/black-tulip-update/black-tulip-update.pdf> accessed 27 October 2013

[953] Ibid.

[954] Neal Hindocha and Eric Chien, 'Malicious Threats and Vulnerabilities in Instant Messaging, Symantec Security Response White Paper, 2003' <https://www.symantec.com/avcenter/reference/malicious.threats.instant.messaging.pdf> accessed 2 May 2016, p15; the software to enable MITM attacks in this way is readily available, see for example the SSLsplit package <http://tools.kali.org/information-gathering/sslsplit> accessed 29 May 2016

[955] See https://www.documentcloud.org/documents/785152-166819124-mitm-google.html accessed 27/oct/13

6.6.3 Packet Injection – Man On The Side (MOTS) attacks

The way data is broken into packets was described in Chapter 2. A data packet has everything in it needed to ensure that it reaches its destination. Data packets have sequence numbers in order to ensure that the data spread across them can be reconstructed. However, the Internet Protocol has a weakness caused by its ability to ignore duplicate packets. If two packets with the same sequence number arrive, only the first will be used.

Packet injection is a technique whereby packets can be sent to the receiver in the hope that they arrive before the real packet. For example, when a user browses to a website, the browser sends a GET request to ask the remote server to send a page. The remote server will do so, sending the page as a series of packets. If an adversary can monitor the GET request being sent by the user's browser, they can insert a packet with the relevant first sequence number. If the user's browser receives this packet first, the real one arriving later is totally ignored.

This research found that the packet injection technique is used in one of two ways. First, it is used by China's firewall to disrupt communications. Here, the firewall injects a reset packet which will cause the user's browser to give an error and not the desired web page. Second, as indicated by papers revealed by Snowden in 2013, it can be used to send redirect requests to the user's browser. This technique, which is referred to as Quantum Insert[956] works because web servers can legitimately send redirect requests to users' browsers, for example to indicate that a web page has moved. An example of how this might be used is as follows. Bob browses to Alice's website for some purpose. His browser issues a GET command in the usual way. The security forces use Quantum Insert to redirect Bob's browser to Hotmail. On receiving the redirect Bob's browser now connects to Hotmail and issues a GET command. Bob happens to be a Hotmail user. His browser now automatically

---

[956] 'Deep Dive into Quantum Insert' (*Fox IT*, 20 April 2015) <https://blog.fox-it.com/2015/04/20/deep-dive-into-quantum-insert/> accessed 25 January 2017

sends across any Hotmail cookies stored from previous sessions. These cookies may include Bob's Hotmail userid and other information which can now be surveilled by the security forces. The security forces now have Bob's IP address and, potentially, details of his Hotmail account.

Quantum Insert relies on the ability to inject packets that beat the genuine packet back to the user's browser. For this to be practical the injectors must be located on high speed Internet links, typically within the major CSPs.

6.6.4 Exploiting fundamental weaknesses in encryption

Encryption has always caused concern for law enforcement agencies. In 1993, the US introduced the Escrowed Encryption Standard (EES) based on a cipher known as Skipjack which was created by the NSA. Devices known as the Clipper chip and Capstone chip implemented EES in hardware. The system worked by the government receiving a copy of the unique key embedded in each chip at manufacture.[957] The Standard was eventually abandoned and in any event would only have been of use if no other encryption devices or products could be used.

Therefore, given the variety of encryption products which are generally available, governments need some other way to gain access to encrypted content. Although MITM attacks can succeed they do so by fooling a client system into opening an encrypted communication with the intercepting third party rather than breaking the encryption.

However, documents released by Snowden regarding project BULLRUN indicated that the NSA had spent 10 years leading an 'aggressive, multi-pronged effort'[958] to break encryption and defeat 'network security and

---

[957] Matt Blaze, Protocol Failure in the Escrowed Encryption Standard, 20 August 1994 <http://www.crypto.com/papers/eesproto.pdf> accessed 25 May 2016

[958] BULLRUN (undated) <https://search.edwardsnowden.com/docs/BULLRUN2014-12-28nsadocs> accessed 22 May 2016

privacy'.[959] Although no definite information is given, Snowden's documents suggest that a mixed method is adopted, including Computer Network Exploitation (CNE), collaboration with other agencies, use of high-performance computers and advanced mathematical techniques. The NSA considered the BULLRUN project to be so sensitive that even the knowledge of the possibility must be heavily restricted.[960]

One outcome of BULLRUN was the modification of a key component of encryption systems. Modern encryption typically relies on the generation of random numbers in order to create the encryption keys. A report in the Press suggested that the NSA had created flawed random number generator which was incorporated by RSA[961] into their security products.[962] Allegedly, this was a modification to the Dual Elliptic Curve Deterministic Random Bit Generator (Dual_EC_DRBG) which was one of four random number generators authorised by the National Institute of Standards and Technology (NIST). This revelation was considered so serious that NIST removed the random number generator from its set of recommended products due to its own investigation and public opinion.[963] The random number generator was set as the default in RSA's own widely used BSafe library allegedly when RSA received a large

---

[959] BULLRUN CoI briefing sheet (undated) <https://search.edwardsnowden.com/docs/BULLRUNCoI–BriefingSheet2013-09-05nsadocs> accessed 22 May 2016

[960] Ibid.

[961] RSA has multiple related meanings. RSA is formed from the initials of Ron Rivest, Adi Shamir and Leonard Adelman who pioneered public key cryptography; as a company, RSA Security produce cryptographic libraries.

[962] Joseph Menn, 'Exclusive: Secret contract tied to NSA and security industry pioneer', (*Reuters*, 20 December 2013) <http://www.reuters.com/article/2013/12/20/us-usa-secuity-rsa-idUSBRE9BJ1C220131220> accessed 22 May 2016

[963] NIST Removes Cryptography Algorithm from Random Number Generator Recommendations, 21/04/14 <http://www.nist.gov/itl/csd/sp800-90-042114.cfm> accessed 22 May 2016

sum of money from the NSA.[964] Weakening the randomness of the generator would make it computationally much easier to work out the seed numbers and therefore, recover the encryption keys. This would certainly fit BULLRUN's aim of defeating Internet privacy.

Another NSA program revealed by Snowden is aimed specifically at VPNs. TURMOIL is described as a passive device designed to extract the encryption key exchange data from a VPN connection. Collected traffic is then fed to the NSA for computational analysis and potentially decryption.[965] By comparison, attempting a brute force attack on the symmetrical Advanced Encryption Standard (AES) is impractical. Researchers who proposed a method to shorten the key recovery time of 128-bit AES-128 theorised that a one trillion core machine capable of processing one billion keys per core per second could still take over two billion years to recover the key.[966] This, plus the fact that the much stronger 256-bit AES-256 is commonly used now, means brute force computational cracking of encrypted information relies on weakening the encryption algorithms or finding other as-yet unpublished flaws. Any encryption product which has been deliberately weakened will provide access not only to governments, but also to criminals and hostile state actors.

6.6.5 Exploiting weaknesses in Tor

This research found that Tor still provides an adequate solution to maintain ones privacy. Slides revealed by Snowden show that the NSA themselves will

---

[964] Daniel Bernstein, Tanja Lange and Ruben Niederhagen, Dual EC: A Standardized Back Door, p2 <https://projectbullrun.org/dual-ec/documents/dual-ec-20150731.pdf> accessed 23 May 2016

[965] David Adrian and others, Imperfect Forward Secrecy: How Diffe-Hellman Fails in Practice, CCS'15 The 22nd ACM Conference on Computer and Communications Security, 12-16 October 2-15 <https://weakdh.org/imperfect-forward-secrecy-ccs15.pdf> accessed 18 December 2016

[966] Dave Neal, 'AES Encryption is cracked' (*the Inquirer*, 17 August 2011) <http://www.theinquirer.net/inquirer/news/2102435/aes-encryption-cracked> accessed 23 May 2016

not be able to routinely de-anonymise Tor users.[967] After analysing Snowden's documents, it is found that the security services have access to some Tor nodes, but this is of little practical use unless they have access to all the nodes in a Tor circuit. As discussed in Section 6.5.2.1, these circuits change with time and can also be changed by the user at any time. Other attack vectors include timing attacks where one compares traffic entering and exiting the network. Yet, the practicalities of this attack method is reduced where Internet traffic is heavy through the various Tor nodes in a circuit, making it hard to determine that data entering really is the same as that exiting. Tor can also be degraded by flooding it with data or advertising slow nodes as fast, causing a bottleneck and potentially dissuading users from using Tor.

However, Snowden revealed evidence of a more active attack on Tor using packet injection. Slides released by Snowden detail a programme called Egotistical Giraffe[968] where Quantum Inserts were used specifically against Tor when websites under surveillance were accessed, redirecting browsers to Hotmail and Yahoo!, and reading any cookies transmitted as a result. These cookies could contain user account details or e-mail addresses, enabling identification of the user concerned. In addition, a programme referred to as FoxAcid was allegedly used with Quantum Insert diverting browsers to the FoxAcid server which would inject malware aimed at de-anonymising the actual user by causing the target computer to bypass Tor and access a server operated by the FBI. This malware caused the target computer to send its MAC address and IP number to the FBI server. This attack worked due to a

---

[967] Tor Stinks, June 2012 <https://search.edwardsnowden.com/docs/TorStinks2013-10-04nsadocs> accessed 29 May 2016

[968] Tailored Access Operations, 'Peeling Back the Layers of Tor with Egotistigal Giraffe', <https://www.eff.org/files/2014/04/09/20131004-guard-egotistical_giraffe.pdf> accessed 25 January 2017

flaw in the version of Firefox used by Tor at that time. This exploit was used to uncover a hidden service[969] hosting child pornography.[970]

6.6.6 Computer Network Exploitation (CNE)

More generally, ISPs themselves are vulnerable. Documents revealed by Snowden and published by Der Spiegel[971] indicate the existence of an operation by GCHQ to gain access to BICS, a Belgacom subsidiary. The aims of the operation were to gain CNE access to Belgacom's core routers in order to carry out MITM attacks against roaming smartphones,[972] to '[e]xpand collection and capability to enable better exploitation of Belgacom',[973] identify key staff[974] and map the Belgacom network,[975] and 'investigate VPN links …

---

[969] Hidden servers are those only accessible via Tor using special DNS entries within Tor itself; they use the .onion domain which does not exist outside of Tor. A well known example was Silk Road which was closed down by the FBI after its owner was traced as a result of using normal email accounts. These hidden services form what has become popularly known as the Dark Web. See United States of America v Ross William Ulbricht

[970] Kevin Poulsen, 'FBI admits is controlled Tor servers behind mass malware attack', (*Wired*, 13 September 2013) <https://www.wired.com/2013/09/freedom-hosting-fbi/> accessed 28 May 2016

[971] 'Britain's GCHQ Hacked Belgian Telecoms Firm' (*Spiegel Online*, 20 September 2013) <http://www.spiegel.de/international/europe/british-spy-agency-gchq-hacked-belgian-telecoms-firm-a-923406.html> accessed 28 May 2016

[972] GCHQ Network Analysis Centre, Mobile Networks in MyNOC World, slide 9 <https://search.edwardsnowden.com/docs/MobileNetworksinMyNOCWorld2014-12-13nsadocs> accessed 28 May 2016

[973] Ibid., slide 11 <https://search.edwardsnowden.com/docs/MobileNetworksinMyNOCWorld2014-12-13nsadocs> accessed 28 May 2016

[974] Ibid.

[975] Ibid.

to other telecoms providers'.[976] This is an example of state sponsored CNE aimed specifically at gaining access to foreign networks.

In addition to the above, other examples are found including the use of zero-day exploits against targets. A zero-day exploit is the use of a vulnerability in software or hardware before that vulnerability is known and therefore, before it can be patched.[977] FoxAcid, or similar exploits could be used to insert zero-day malware into a target computer. There is no protection from such an exploit because until it is revealed, virus scanners and detection software cannot be updated to check for the vulnerability. Bilge and Dumitras determined that the average lifetime of such exploits is 312 days during which criminals and state actors alike can continue to use exploits undetected.[978] Hence, there is a clear implication on privacy. For example, if such an exploit were to install a key-logger, for example then everything typed could potentially be fed to an adversary, bypassing any privacy protections in place. Alternatively, access to the filesystem could give access to one's private key which could then be used to decrypt any encrypted communications.

6.7 Conclusion

From a technical point of view, it is difficult to see how privacy can be reliably maintained when faced with state actors with significant resources and access to techniques like those of the US and the UK. Once again, this is a clear indication that when compared to China, the US and the UK are not so

---

[976] Ibid.

[977] An extreme example of a zero-day exploit is Stuxnet which was used to physically destroy centrifuges at an Iranian nuclear processing facility. Although not initially Internet delivered it used zero-day exploits in Microsoft Windows. See Ralph Langner, 'Stuxnet: Dissecting a Cyberwarfare Weapon', IEEE Security & Privacy, May/June 2011, pp 49-51

[978] Leyla Bilge and Tudor Dumitras, 'Before We Knew It: an Empirical Study of Zero-Day Attacks In The Real World', CCS '12: Proceedings of the 2012 ACM Conference on Computer and Communications Security, October 2012.

different where Internet privacy is concerned. However, the argument that governments need to be able to invade the privacy of terrorists in order to keep us safe is a powerful one. Another equally powerful is the argument presented by governments is that if one could truly secure one's communications content and metadata from the security agencies, this dramatically weakens their ability to fight terrorism and crime.

The Internet Engineering Task Force (IETF) defines pervasive monitoring as an attack and will work to mitigate it.[979] Therefore, it is very likely that future technical efforts to maintain Internet privacy will be proposed. Encryption is part of the privacy battleground. Efforts outlined above to increase the use of encryption on the Internet are met with potential legislation to weaken or provide back-door access to encrypted communications. China goes one step further and can now block encrypted communications. Encryption remains a viable mechanism to protect content privacy in the US and the UK, but this is threatened by legislative moves. In addition to this, new technologies threaten to dramatically decrease the time taken to computationally break encryption.[980] The Internet has become a technology battleground, with methods of defeating encryption pitted against methods to protect it.

Yet, finding the terrorist is a complex problem. An IP address is not a reliable way to prove that someone sent a communication or is communicating with someone else. Tracing what IP address connects to where does not necessarily show who is communicating with whom. An IP address by itself may only show who pays the bill for the relevant ISP service, and where services such as VPNs or Tor are used the recorded IP address may not even be on the same continent.

---

[979] Stephen Farrell and Hannes Tschofenig, Pervasive Monitoring is an Attack <https://tools.ietf.org/html/rfc7258> accessed 23 December 2012

[980] Amy Nordrum, Quantum Computer Comes Closer to Cracking RSA Encryption, IEEE Spectrum, 3 march 2016 <http://spectrum.ieee.org/tech-talk/computing/hardware/encryptionbusting-quantum-computer-practices-factoring-in-scalable-fiveatom-experiment> accessed 19 October 2016

As has been shown in this chapter, given the resources available to intelligence agencies tapping the Internet is relatively straightforward. If this tapping is done at sufficiently numerous, tactically relevant locations, then the whole Internet actually could become a surveillance mechanism. The issue then becomes not how to acquire the communications, but how to analyse the sheer quantity of data this would produce in order to produce any useful intelligence.

This chapter also demonstrated methods of maintaining Internet privacy. None are perfect when faced with the programmes revealed by Snowden, but they are able to secure the content of communications and, to a great extent also the metadata.

As described in Chapter 2, the Internet was likened to the road network with multiple paths where traffic is free to choose any path, and choke points through which everything must pass if travelling between countries. Although the Internet today is no longer so simple, it still has multiple paths and choke points. Also, information can be held at any point at the edge, or even in what may be considered the centre. Large datacentres store data which may then be described as being in the cloud and people may have no idea as to where their data actually is at any given time. The Internet of Things is causing an explosion in the amount of data being pushed into the cloud, data which when collated may well form a very detailed profile about a family or an individual. In a surveillance society, all of this data may be accessible by the State, or by all States.

Turning the Internet into a global surveillance machine puts everyone under surveillance regardless of guilt. Currently, no other technology offers this.

This page is intentionally left blank

Chapter 7: Recovering Internet privacy: reflection and discussion

7.1 Introduction

This research initially set out to answer the research question: Is Internet privacy dead? In relation to this primary research question, two sub-questions were also posed: have the US and the UK reached the level of China with regard to the invasion of Internet privacy; and what measures can be taken to prevent mass Internet surveillance from destroying Internet privacy?

So far, this research has reviewed the meaning of privacy in an Internet context and focused on the protection of one's personal information. The structure of the Internet has been explained in order to pinpoint and demonstrate where and how easily privacy may easily be invaded. Further, Internet privacy protections and violations in a set of three chosen jurisdictions – the US, the UK and China – were examined and discussed in Chapters 3, 4 and 5 respectively. The research found that in each case, there is clear evidence to show that privacy takes a back seat to surveillance, regardless of the reason for that surveillance. Methods of protecting Internet privacy and an analysis of the Snowden revelations surrounding increasing government mass Internet surveillance programmes was discussed in Chapter 6.

The aim of this chapter is to build on the research findings from the previous chapters and propose answers to the specific research questions.

7.2 The US, the UK and China: A comparative introspection

Have the US and the UK reached the level of China with regard to the invasion of Internet privacy? As was discussed in Chapter 5 China has a highly developed Internet surveillance system and firewall which is able to block access to content, to monitor content for keywords, and to block encrypted communications. Its surveillance system is a mixture of technological and human monitoring. China does this in order to censor information arriving from outside the country as well as to monitor what citizens such as micro-bloggers are writing online.

From a technical perspective, the Chinese firewall is effective because at that level, it becomes physically impossible to reach an external website which is blocked. Additionally, China has evolved its technology to enable it to block encrypted communications, thus preventing people inside China from accessing services such as VPNs, Tor or any other service offering E2EE.

China blocks social media websites, but in turn offers its own versions of these. It was reported that Weibo logged 222 million active users in September 2015[981] with WeChat recording 806 million active users per month in the second quarter of 2016.[982] These Chinese social media websites are popular and active, although again the censors can easily have material removed and accounts closed down with ease. Providing such in-country services with little other choice also increases China's ability to monitor what it's citizens are doing online.

China's real name policy when combined with blocks on encryption and State surveillance means it is hard to maintain any form of anonymity on the Internet. Internet privacy in China is thus dead. For this reason, China is presented as a worse-case scenario in terms of Internet privacy protection.

However, although China appears to be a rights-oppressive state with an impressive country-wide Internet censorship and surveillance system, it is increasingly hard to hold China up as a pariah when the West invests in ever new ways to surveil its own population as well as that of the entire Internet. Where China may carry out intensive Internet surveillance, it does so for reasons including censorship and social stability; when one considers its desire to block pornography not all of this censorship is bad. The West increasingly desires to surveil the Internet in order to find terrorists or to thwart serious crime. While this may be laudable, the fact remains that both the US

---

[981] CIW Team, Weibo Search Users Insight 2015 <https://www.chinainternetwatch.com/16366/weibo-search-users-insights-2015/> accessed 27 December 2012

[982] CIW Team, WeChat monthly active users reached 806 million in Q2 2016 <https://www.chinainternetwatch.com/18789/wechat-monthly-active-users-reached-806-million-in-q2-2016/> accessed 27 December 2012

and the UK mount mass Internet surveillance. The difference is that with China, everyone is aware of the state's desires and the fact that censorship is happening. Although each jurisdiction has enshrined surveillance in laws, the US and UK have attempted to hide the shear breadth of their Internet surveillance operations and capabilities, in part only revealed as a result of the 2013 Snowden revelations. Chapter 6 discussed the Snowden revelations and set out how surveillance programmes mounted by both the US and the UK apparently sought to gather as much information as possible via Internet taps and partnerships with major players. In addition to this, the laws and surveillance mechanisms in both the US and the UK were examined in Chapters 3 and 4, respectively, and in both cases, these act extraterritorially.

The similarities are stark. China can control its Internet because it controls all the gateways connecting China to the wider, global Internet. In the US and the UK these gateways are not government owned or controlled but are operated by for-profit corporations. This may appear to be a fundamental difference, yet, the US and the UK both mounted surveillance operations in conjunction with these for-profit corporations, either by compelling them or by implementing laws that require them to provide surveillance capabilities, such as CALEA in the US and now the Investigatory Powers Act in the UK. In reality, it means that all three jurisdictions have similar surveillance capabilities regardless of the actual ownership of the infrastructure.

However, China's surveillance is at its borders and inwards. The situation with the US and the UK is dramatically different in that each State has major global Internet infrastructure carrying a very high proportion of the world's Internet traffic. As was explained in Chapter 6 even where countries in the Southern Hemisphere are communicating with each other there is a good chance the communications path will traverse the US, the UK or, indeed, both. Each State has laws in place permitting extraterritorial surveillance, which includes surveillance of foreign Internet traffic passing through its gateways. Mass Internet surveillance in the US under EO12333 and FAA 702, and in the UK under Tempora are clear indications that the Internet surveillance capabilities of these two States far exceed that of China.

The use of encryption, put forward in Chapter 6 as a way to protect privacy of the content of communications as well as some of the metadata can now be blocked by China. It may seem that China has the upper hand when it comes to the invasion of Internet privacy if all content is accessible because encryption cannot be used. However, MITM provides one way to maintain access to encrypted communications. Furthermore, the weakness inherent in digital certificates and the possibility that governments will compel CAs to produce certificates such that the intelligence agencies can set up servers that pretend to be those of legitimate providers means that there are still ways to access encrypted material. Additionally, the arsenal of techniques amassed by the intelligence agencies which may be used in Internet surveillance may not yet be fully revealed by the Snowden revelations. Again, these three jurisdiction are not that different when it comes to the invasion of Internet privacy. China defeats encryption by making it impossible to use – the US and the UK do so by employing a range of technical measures.

So, have the US and the UK reached the level of China with regard to the invasion of Internet privacy? If they have, then given there is no Internet privacy in China it means that Internet privacy in general is indeed dead. However, China's control of the Internet is total, whereas in the US and the UK there are still effective methods of maintaining privacy on the Internet. For example, the use of VPNs and Tor are still possibilities. While these remain viable, although it may appear that in some cases the US and the UK have exceeded the invasiveness of China, it is not in totality. Therefore, it is proposed that the US and the UK have come close to China's level of invasion of Internet privacy but as will be examined next the situation is not yet completely lost.

7.3 The protection of Internet privacy

The principal issue dealt with in this research is mass Internet surveillance. Although brought into public view by Snowden, the issue of mass Internet surveillance was discussed several years before that. This type of surveillance is flawed. It is inevitable that data mining the large datasets created by mass Internet surveillance will generate large numbers of false-positives and

negatives, resulting in actions being taken against large numbers of innocent people with little actual chance of finding the terrorists or criminals.[983] Looking for a needle in a haystack is a popular analogy to use, but Schneier warns that when examining the haystack to find a needle, the thing not to do is keep adding hay.[984] Yet, the strategy to collect all available data employed by the security agencies is doing exactly that. Because terrorists make every effort to merge into the crowd, one is then faced with finding the right needle in a great many needles.[985] This is wholly disproportionate and must therefore fail the necessity test of the ECHR. Furthermore, if the action were considered arbitrary it must also fail Art 17 of the ICCPR. In any event the effectiveness of this method of surveillance is in doubt. For example, in an investigation into 225 cases where individuals were charged with some form of terrorism related crime, it is found that bulk metadata collection played a part in a maximum of 1.8% of those cases.[986]

Lessig's regulatory model is centred around what he terms a pathetic dot. This dot has four modalities acting upon it: architecture, market, law and norms. [987] When related to Internet privacy architecture, which Lessig terms 'code' is the Internet itself and includes software agents. However, these modalities can not only regulate but can also protect.[988] Where the pathetic dot represents

---

[983] Ian Brown and Douwe Korff, 'Terrorism and the Proportionality of Internet Surveillance', European Journal of Criminology 6(2), 2009, 125

[984] Bruce Schneier, Data mining for terrorists, 09/03/06 <https://www.schneier.com/blog/archives/2006/03/data_mining_for.htm> accessed 14 October 2016

[985] Fred H Cate, 'Government Data Mining: The Need for a Legal Framework', 43 Harv. C.R.-C.L. L. Rev. 435, 2008, 473

[986] Peter Bergen and others, Do NSA's bulk surveillance programs stop terrorists?, New America Foundation, January 2014, p4 <https://static.newamerica.org/attachments/1311-do-nsas-bulk-surveillance-programs-stop-terrorists/IS_NSA_surveillance.pdf> accessed 12 December 2015

[987] Lawrence Lessig, *Code version 2.0*, (Basic Books, New York, 2006) 121-123

[988] Ibid., 234

Internet privacy Lessig's model thus shows that each modality can regulate Internet privacy and also protect it. The ability of the law to protect privacy and also to regulate its invasion has been examined in previous chapters. The architecture of the Internet has been examined in Chapter 2 and in more depth in Chapter 6 and the laws and regulations in the three chosen jurisdictions were covered in Chapters 3, 4 and 5. These are discussed further, below. The role of social norms and the market and how these may aid Internet privacy are examined next.

7.3.1 Increasing the awareness of informational privacy

We live in societies and are subject to the norms determined by those societies. These norms may define what actions are right and what are wrong, theft for example.[989] Norms may also define a demarcation between public and private, restricting access to an individual in a private space,[990] thus, privacy itself is a social norm.

Lessig points out that norms on the Internet are different from those local norms that one is subjected to.[991] People may thus act differently when using the Internet because the norms differ. The CEO of Facebook indicated that people have become comfortable in sharing information more openly with others, and that this is a social norm which has been built over time.[992] Where one would not tell strangers one's personal details one may be content with sharing personal information generally on social networks simply because this follows the norm. Similarly, one would not expect to pass personal information to a shop keeper on making a purchase. Yet, on an Internet store one may

---

[989] Ibid., 11

[990] Ferdinand David Schoeman, *Privacy and Social Freedom*, (Cambridge University Press, 1992) 15

[991] Lessig (n 987) 19

[992] Amitai Etzioni, 'The Privacy Merchants: What Is To Be Done?', 14 U. Pa. J. Const. L. 929, 952 (2012), 938

need to supply a lot of personal information in order to create an account before a purchase can be made.

People are mostly aware that personal information that they provide to websites on the Internet is collected but they may not be aware of the potential for invasions of privacy this data provides or even how their personal information will be used.[993] Privacy policies and associated practices can change at any time with notification typically only announced in the policies themselves.[994] These policies are often ignored, not necessarily because they are difficult to read but because people just do not want to read them.[995] In addition functionality can be changed which result in one's personal information being treated in a different and potentially more invasive way. For example, Facebook changed its privacy settings in May 2010 following protests from users who found that previous changes caused confusion as to what information was public.[996] Those setting still proved complex. In September 2010, a girl advertised her 15th birthday party as a Facebook event. Intending to only invite her friends, the event was actually marked as public. As a result, some 21,000 people ticked the box to say they would attend.[997]

While we may be willing to share our personal information with others via social media websites, for example, the Snowden revelations made it clear that governments can and will tap into that information. Facebook, which gathers a large amount of personal information from its users and is designed

---

[993] Ibid., 929

[994] Privacy policies can be hard to understand and take time to read, see Outlaw 'Average privacy policy takes 10 minutes to read, research finds' <http://www.out-law.com/page-9490> accessed 18 January 2011

[995] Daniel J Solove, *The digital person: technology and privacy in the Information Age*, (New York University Press, New York, 2004), 82

[996] See BBC news item <http://www.bbc.co.uk/news/10167143> accessed 4 December 2010

[997] See <http://www.bbc.co.uk/news/uk-england-beds-bucks-herts-11376350> accessed 4 December 2010

such that people use their real names[998] was named as one company that is a key provider of information to the US government under the PRISM program which was discussed in Chapter 6.

Set against this background it is clear that people are becoming more aware of the issues of mass Internet surveillance. The press coverage of the Snowden revelations has resulted in change. In 2015, a report produced by the Pew Research Center stated that 30% of US adults had 'taken at least one step to hide or shield their information from the government.'[999] The 2016 TRUSTe / National Cyber Security Alliance consumer privacy index reports for the US and UK show that 44%[1000] of US and 50%[1001] of UK citizens share the opinion that Internet privacy will improve as consumer awareness improves. Both surveys show that the majority of people are concerned about informational privacy while awareness of how their information is used is in the minority. In addition, both surveys indicate that the majority of people will avoid companies that do not protect informational privacy.

Education here leads to choice and changes to the social norms governing our use of the Internet. One may choose to share less information or to take greater care when sharing. One may choose to use privacy enhancing tools such as VPNs or Tor, and/or to move to using E2EE. In this way it can also influence the market in that software products implementing E2EE may become more mainstream. As people take more notice of privacy settings and of their use of personal information in general this has the potential to shift the

---

[998] Amitai Etzioni (n 992) 933

[999] Martin Shelton and others, Pew Research Center, Americans' Privacy Strategies Post-Snowden, 16 March 2015 <http://www.pewinternet.org/files/2015/03/PI_AmericansPrivacyStrategies_0316151.pdf> accessed 20 October 2016

[1000] 2016 TRUSTe/NCSA Consumer Privacy Infographic – US Edition < https://www.trustarc.com/resources/privacy-research/ncsa-consumer-privacy-index-us > accessed 6 September 2017

[1001] 2016 TRUSTe/NCSA Consumer Privacy Infographic – GB Edition < https://www.trustarc.com/resources/privacy-research/ncsa-consumer-privacy-index-gb > accessed 6 September 2017

norm away from the Facebook model outlined above to one where people are less comfortable sharing personal information, thus providing greater informational privacy and giving us greater autonomy.

One crucial question remains. One must ask *why* we should change our habits because of mass Internet surveillance. It could be argued that we have already changed our habits in order to use the Internet as we now more freely communicate and share information. Yet, the Internet, and more specifically the Web, have developed to benefit mankind as a whole. Why, then, should we now use it less because of surveillance? Of course, we should be able to use it to our benefit in whichever way we chose.

7.3.2 Technical challenges to mass Internet surveillance

Awareness of the threats of mass Internet surveillance can also play a part in major changes to the location of personal information and how it is handled by key companies. The move to cloud based services has resulted in data, including personal information being sent to data processing facilities in foreign jurisdictions. If such data moves between the EU and the US the data will pass across transatlantic cables and thus be subject to interception under Upstream and Tempora. To combat this providers such as Microsoft[1002] and Amazon[1003] are building data centres within the EU. These moves are predominantly to solve the issues of exporting personal information outside of the EU, but they have had an effect on law enforcement access to data. This can be illustrated by a 2014 case where the US Government had used the SCA to attempt to compel Microsoft to produce e-mails from a Hotmail account physically hosted in Ireland. Here, a search warrant had been issued covering

---

[1002] Peter Bright, 'Microsoft to offer UK–based Azure, Office 365 from late 2016' (*Arstechnica*, 11 November 2015) <http://arstechnica.co.uk/information-technology/2015/11/microsoft-to-offer-uk-based-azure-office-365-from-late-2016> accessed 30 May 2016

[1003] Daniel Robinson, 'Amazon Web Services to open first UK data centre post Safe Harbour ruling' (*V3*, 6 November 2015) <http://www.v3.co.uk/v3-uk/news/2433779/amazon-web-services-to-open-first-uk-data-centre-post-safe-harbour-ruling> accessed 30 May 2016

premises 'owned, maintained, controlled, or operated'[1004] by Microsoft, regardless of their location. Microsoft appealed, but the US District Court for the Southern District of New York agreed with the original ruling.[1005] Microsoft then appealed to the Second Circuit and gained high level support by way of amicus briefs from Amazon, Apple and the Irish Government, among others.[1006] The Court found in Microsoft's favour, concluding that the SCA warrant could not be used to force Microsoft to produce the relevant e-mails from the Dublin server, and reversing the decision of the District Court.[1007]

Microsoft has built data centres in Germany where all customer data will be under the control of a data trustee which is a subsidiary of Deutsche Telekom. This means that the data will no longer be controlled by Microsoft, or any other US company, further excluding it from the reach of the SCA. Microsoft Cloud Germany ensures that personal data stored in its cloud product remains in Germany and is controlled by the data trustee. Microsoft themselves have no right of access to servers which hold customer data without the supervision of the data trustee.[1008]

The mass surveillance revealed by Snowden could have other effects on the structure of the global Internet. For example, Brazil's Internet connections are currently routed via Florida in the US as was illustrated in Chapter 6. In 2014,

---

[1004] Search and Seizure Warrant, Exhibit A, Attachment A <http://digitalconstitution.com/wp-content/uploads/2014/11/government-warrant.pdf> accessed 30 May 2016

[1005] In re Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp., No. 14-2985-CV, 2014 WL 4629624 (S.D.N.Y. Aug 29, 2014)

[1006] See <http://digitalconstitution.com/about-the-case/> accessed 30 May 2016

[1007] In the matter of a Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corporation, United States Court of Appeals for the Second Circuit, July 14, 2016, 42

[1008] Microsoft Cloud Germany <http://download.microsoft.com/download/6/1/3/613C9ECB-9167-4EF5-B131-3BAD8D8A126C/Microsoft_Cloud_Germany_Datasheet.pdf> accessed 27 December 2016

Brazil and the EU began planning to deploy a submarine cable running under the Atlantic to Spain in order to avoid the US completely.[1009] Brazil may have engaged in political spin because the cable was actually announced in September 2012 before the 2013 Snowden revelations.[1010] However, the fact remains that this is an example of Internet infrastructure being deployed which bypasses both the US and the UK.[1011]

The above section gives a clear indication that the location and storage of personal information and, potentially the structure of the Internet itself is changing as a result of the threat of mass Internet surveillance.

7.3.3 Legislative challenges to mass Internet surveillance

As investigated above increased awareness of the risks of mass Internet surveillance has the potential to reduce the amount of personal information which we share, but the architecture of the Internet itself still poses a risk. Software suppliers have produced products with E2EE as a default and awareness of the issues can increase the update of these. Encryption is an effective way to secure one's content but even where encryption is used the metadata is still at risk. As a solution, Tor does provide a greater degree of privacy protection than E2EE because it masks the metadata and routes between systems and even continents before accessing the target system. However, as was discussed in Chapter 6 Tor is not a mainstream product and does not give the same user experience when using media rich websites.

[1009] Robin Emmott, 'Brazil, Europe plan undersea cable to skirt U.S. spying' (*Reuters*, 24 February 2014) <http://www.reuters.com/article/us-eu-brazil-idUSBREA1N0PL20140224> accessed 27 December 2016

[1010] IslaLink will build a submarine cable between Europe and America – 12 Sept 2012, see <http://www.islalink.com/en/islalink-will-build-a-submarine-cable-between-europe-and-america.html> accessed 27 December 2016

[1011] The cable route can be seen via Telegeography's Submarine Cable Map <http://www.submarinecablemap.com/#/submarine-cable/ellalink> accessed 27 December 2016

Clearly, these methods alone cannot provide security from the threats to autonomy and informational privacy posed by mass Internet surveillance. It is therefore necessary to investigate how the law can help. As was shown in previous chapters the law can enable mass Internet surveillance but can also provide stronger privacy protections. Of equal importance the law can also regulate the intelligence agencies. These laws have evolved through key court cases and, in the case of the UK from the jurisprudence of the ECHR. However, generally speaking the protections provided by those laws act inwardly or act to protect only the citizens of a given jurisdiction. This allows extraterritorial surveillance which paved the way for the mass Internet surveillance carried out by programmes such as Upstream and Tempora. Because of this one needs to look to International law.

Turning to international law privacy is enshrined in ICCPR Art.17 which was covered in Chapter 2. Art.17 includes two tests: whether interference with privacy is arbitrary; or unlawful. While the legality of interference with privacy may be defined in domestic laws, whether that interference is arbitrary needs further analysis. The UN Human Rights Council held the view that in order to pass the *arbitrary* test, interference, even if lawful, must be reasonable given the circumstances.[1012] Referring to the *Weber* judgment the Human Rights Council reiterated that the very existence of mass Internet surveillance is an interference with privacy and that states would need to demonstrate that this is neither unlawful nor arbitrary.[1013] It also stressed that even where an interference is in accordance with national law it may still fail the tests of Art. 17 if that law is incompatible with the ICCPR. The Committee made a number of recommendations regarding mass Internet surveillance which can be summarised as follows:

[1012] CCPR General Comment No.16: Article 17 (Right to privacy) The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation, Adopted at the Thirty-second Session of the Human Rights Council, on 8 April 1988, 4

[1013] Office of the High Commissioner for Human Rights, The right to privacy in the digital age, A/HRC/27/37, 30 June 2014, 20

- Surveillance must necessary, carried out for a legitimate aim and must have some chance of meeting its goals.[1014]
- It must be proportionate to that aim including the need for it to be the least intrusive method available.[1015]
- The law must be accessible meaning it must be both published and detailed such that a person can know which agencies can carry out surveillance and can foresee the consequences of that surveillance.[1016]
- There must be effective safeguards and independent oversight to prevent abuse of surveillance.[1017]
- There must be an effective remedy for violations of Art. 17.[1018]

The UN has become increasingly outspoken on the issue of mass Internet surveillance. Emmerson[1019] pinpointed that merely stating that mass surveillance can assist in the fight against terrorism does not provide justification for its use with regard to human rights. He further stated that '[t]he fact that something is technically feasible, and that it may sometimes yield useful intelligence, does not by itself mean that it is either reasonable or lawful'.[1020] He also called for all states operating mass Internet surveillance programmes to produce a 'detailed and evidence-based public justification for the systematic interference with the privacy rights of the online community'.[1021] Both the US and the UK have received unfavorable comments from the

---

[1014] Ibid., 23

[1015] Ibid.

[1016] Ibid., 28

[1017] Ibid., 37

[1018] Ibid., 39-41

[1019] Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism

[1020] Ben Emmerson, Promotion and protection of human rights and fundamental freedoms while countering terrorism, UN General Assembly, A/69/397, 23 September 2014, 11

[1021] Ibid., 63

Human Rights Council which expressed concern at mass communications surveillance and lack of oversight and safeguards. In both cases the Committee called for measures to be taken to ensure that surveillance meets the requirements of Art. 17 'regardless of the nationality or location of the individuals whose communications are under direct surveillance',[1022] clearly targeting the extraterritorial nature of Upstream and Tempora.

Putting privacy further on the UN's agenda, the UN Human Rights Council appointed a Special Rapporteur in June 2015 with a mandate[1023] to investigate best practice and obstacles to privacy and, in particular, to report on alleged violations of UDHR Art. 12 and ICCPR Art. 17.[1024]

A common analogy put forward when one is attempting to find one person in the crowd is that one is looking for a needle in a haystack. However, the necessity test should not be whether the aim of finding a needle in a haystack is a legitimate one; one needs to measure the impact on the whole haystack caused by the finding of that needle.[1025] Given the successes or failures of mass Internet surveillance regimes are mostly hidden from public scrutiny by national security laws, it is hard to see how States can still justify these programmes under the ICCPR. Cannataci was particularly critical of the UKs Investigatory Powers Act, inviting the government to stop 'setting a bad example to other States'[1026] by continuing to introduce legislation promoting mass Internet surveillance.

[1022] CCPR/C/USA/CO/4 22(a) and CCPR/C/GBR/CO/7 24(a)

[1023] UN Special Rapporteur on the right to privacy <http://www.ohchr.org/EN/Issues/Privacy/SR/Pages/SRPrivacyIndex.aspx> accessed 12 October 2016

[1024] Ibid., (g)

[1025] Office of the High Commissioner for Human Rights, The right to privacy in the digital age, A/HRC/27/37, 30 June 2014, 25

[1026] Joe Cannataci, Report of the Special Rapporteur on the right to privacy, UN Human Rights Council, A/HRC/31/64, 24 November 2016, 38

7.4 Is Internet privacy dead? The regulation of mass Internet surveillance

The fundamental concern with mass Internet surveillance is that it puts everyone's informational privacy at risk. Programmes such as PRISM, Upstream and Tempora aim to collect massive amounts of personal information as it is gathered by companies or flows across key Internet pathways. This personal information is gathered regardless of whether the people concerned are suspected of any wrongdoing. This is inconsistent with principles of autonomy, taking away our freedom to choose courses of actions or to choose what is known about us by others as was covered in Chapter 2.

A key question is how surveillance laws and intelligence agencies are scrutinised by the courts. The effects of this has been seen at supranational level where the CJEU invalidated the DRD as was examined in Chapter 4. Subsequent legislation in the UK permitted data retention to continue. Changes in the law in the US terminated Section 215 telephone metadata collection in 2015, but Upstream collection under FAA702 persists. However, effective oversight combined with a method by where people can complain of privacy violations is crucial if states are to comply with their responsibilities under Art. 17 of the ICCPR.[1027] It is also vital that laws are accessible such that people know what laws can affect them and how. A key tribunal ruling in the UK showed that this mechanism can be effective and this is examined next.

7.4.1 Investigatory Powers Tribunal and PRISM, Upstream and Tempora

It is clear that regional courts can have an effect on the law in the UK. ECtHR rulings which have resulted in new legislation in the UK were examined in Chapter 4. However, in 2015 the IPT reached a landmark decision. As a result

[1027] CCPR General Comment No.16 (n 1012) 6

of the Snowden revelations several claimants[1028] brought cases against the security and intelligence agencies.[1029] The allegations made were that PRISM, Upstream and Tempora[1030] breached ECHR Art. 8.

Discussing PRISM and Upstream the tribunal noted that these are lawful and covered by FAA702 and EO12333 which were discussed in Chapter 3. However, as was discussed in Chapter 6 and as argued by the claimants information intercepted under the PRISM / Upstream programs could contain communications from the UK and if this is then shared with the UK under the Five Eyes agreement the UK intelligence agencies could receive intercepted material from private individuals in the UK without the safeguards contained in RIPA.

The security and intelligence agencies claimed that provisions in various Acts (Security Service Act 1989, Intelligence Services Act 1994, Counter-Terrorism Act 2008) cover for such use of material. However, although these Acts set limits on what the agencies are permitted to do they do not explicitly deal with obtaining intercept material from foreign governments. Thus, if the UK made use of US intercept material containing UK personal communications this has no adequate protection and fails the tests of ECHR Art. 8(2).[1031]

The concern that faced the tribunal was that there must not be 'unfettered discretion for executive action'[1032] and that the rules of interference must be clear such that their effect on privacy can be foreseen – if not then it could be

---

[1028] Liberty, Privacy International and Amnesty International in the UK, ACLU, Bytes For All and others

[1029] Investigatory Powers Tribunal case numbers IPT/13/77/H, IPT/13/92/CH, IPT/13/168-173/H, IPT/13/194/CH and IPT/13/204/CH [2014] UKIPTrib 13_77-H

[1030] Note the term Tempora is used here as revealed in the Snowden revelations; as the security and intelligence agencies have not acknowledged its existence the IPT used the term 's.8(4) issue' after RIPA s.8(4)

[1031] Investigatory Powers Tribunal (n 1029) 21

[1032] Ibid., 37(ii)

judged to not be in accordance with the law and thus breach ECHR Art. 8. The issue was resolved when the agencies disclosed information regarding internal processes governing requests to foreign governments for 'unanalysed intercepted communications'[1033] and metadata. Such material would (a) be requested either subject to a RIPA warrant or, (b) if it could not be obtained in that way, for example for technical reasons, the Secretary of State would first decide whether or not that request should be made. In other cases where material is received it is treated as if it were obtained under RIPA.[1034] Although it noted a possible issue with the latter case (b) that RIPA s.16 protection may not apply the IPT concluded on 5 December 2014 that material obtained via PRISM / Upstream did not breach the ECHR Art. 8 rights of UK citizens. However, this 2014 conclusion would be modified two months later.

The tribunal had requested that all parties make further submissions. Further disclosures were made to confirm that RIPA s.16 would be considered by the Secretary of State should such a request be made. However, on the issue of PRISM / Upstream more generally reference to the disclosure made regarding internal procedures was necessary in order for the law to be accessible and safeguards to be known. As this was not public knowledge until the judgment of 5 December 2014 the IPT now concluded that prior to that date 'the Prism and/or Upstream arrangements contravened Articles 8 or 10 ECHR, but now comply.'[1035] For the first time in its history the IPT had found in favour of a claimant in a case brought against the security and intelligence agencies.[1036] Of note, the issue of secret procedures had previously aided the ECtHR to

---

[1033] Ibid., 47

[1034] Ibid.

[1035] Investigatory Powers Tribunal case numbers IPT/13/77/H, IPT/13/92/CH, IPT/13/168-173/H, IPT/13/194/CH and IPT/13/204/CH [2015] UKIPTrib 13_77-H 32

[1036] Investigatory Powers Tribunal report 2011-2015, 3.1 <http://ipt-uk.com/docs/IPT%20Report%202011%20-%202015.pdf> accessed 12/Aug/2017

find against the UK in *Liberty and Others v United Kingdom* which was discussed in Chapter 4.

The second part of the IPTs ruling dealt with Tempora. Operating under RIPA s.8(4) Tempora was described in Chapter 6 as a program to tap submarine cables and retrieve all information flowing across these for later analysis. The respondents made it clear in their submissions that in order to find the needles they must look through the entire haystack of data.[1037]

The questions before the tribunal were whether the use of RIPA s.8(4) could be found to be not in accordance with the law given the issue of determining which communications are external and which are internal; whether the safeguards in RIPA s.16 are sufficient; and whether RIPA stands up against the tests in *Weber*.[1038] The tribunal noted that it is impossible to differentiate between internal and external communications at the point of interception. The interception of external communications is permitted by RIPA s.8(5). RIPA s.5(6) permits such interception to include communications not covered by the warrant should this be necessary in order to carry out that warrant.[1039] Therefore, it found that RIPA s.8(4) lawful.

On the issue of RIPA s.16 the claimants complained that there was no protection for metadata. However, the tribunal found that RIPA s.15 protections would apply here and found no issue regarding the protections provided under RIPA generally.[1040] Technically, if such metadata could not be used then it would not be possible to determine which communications are internal and which external before selecting the external ones for analysis. The tribunal also concluded that the safeguards and the purpose of the surveillance would pass the *Weber* test.

[1037] Investigatory Powers Tribunal (n 1029) 80

[1038] Ibid., 80

[1039] Ibid., 93

[1040] Ibid., 114

The result of these proceedings underlines the government's view that interception operations under PRISM, Upstream and Tempora are lawful. However, the claimants filed an application with the ECHR which is yet to be heard.[1041] Moreover, the case indicates the willingness of the IPT to rule against surveilling agencies if it finds errors in procedure or the law. It underlines the need that the law be accessible to the people governed by it, a requirement set by the ICCPR. However, a case heard by the CJEU would lead to questions regarding mass Internet surveillance from a data protection perspective and this is examined next.

7.4.2 Data protection and the fall of Safe Harbor

One notable casualty of the Snowden revelations was the Safe Harbor agreement between the EU and the US, the very basis of which was found to be flawed in *Maximillian Schrems v Data Protection Commissioner*.[1042] Safe Harbor was discussed in Chapter 4 as a means to continue to allow the transfer of personal information to the US in the face of protective data protection legislation that would otherwise prohibit it.

Schrems was concerned that his personal information was being transferred between Facebook Ireland and the Facebook servers in the US, putting it at risk of surveillance due to the activities of the NSA as revealed in the Snowden revelations. The Irish Data Protection Commissioner rejected his complaint based on the fact that Safe Harbor supposedly provided an adequate level of protection. Schrems took his case to the High Court of Ireland which stated that the 'mass and undifferentiated accessing of personal data is clearly contrary to the principle of proportionality'.[1043] The Court would only accept such surveillance if it were targeted, justified and with appropriate safeguards. However, the Court decided to refer the issue to the CJEU on the basis that it

---

[1041] 10 Human Rights Organisations and others v United Kingdom, App. No. 24960/15, 20 May 2015

[1042] C-362/14 *Maximillian Schrems v Data Protection Commissioner* (Grand Chamber, 6 October 2015)

[1043] ibid., 33

considered Safe Harbor inadequate. The CJEU declared the Commission's Safe Harbour Decision to be invalid, finding that the Commission had merely examined the proposals for the Safe Harbor scheme rather than determined if the domestic laws in the US provided the relevant protection.[1044]

Safe Harbor was replaced by the EU-US Privacy Shield on 12 July 2016. In one respect, the 2013 Snowden revelations made this possible as the US and EU had been in discussion over Safe Harbor since late 2013 because of his revelations.[1045] This new agreement was a result of the US giving assurances that government access to personal information in national security cases would be subject to safeguards and limitations that had not been in place before. However, Privacy Shield is now under threat of legal action. Digital Rights Ireland, the pressure group involved in the downfall of the DRD have lodged an action with the CJEU against the EC. The claim is that the EC made a 'manifest error of assessment'[1046] in determining that the US provides adequate protection of personal information. Another case has also been lodged with the CJEU similarly stating the EC was 'manifestly incorrect'[1047] in determining that Privacy Shield assures adequate protection of personal information.

7.4.3 Threats to mass Internet surveillance

While *Schrems* dealt a fatal blow to Safe Harbor, in his analysis of *Roman Zakharov v Russia*[1048] Cannataci, the UN Special Rapporteur on the right to privacy suggests that this case could potentially do the same to mass Internet

---

[1044] Court of Justice of the European Union Press Release No 117/15, Luxembourg, 6 October 2015

[1045] Martin A Weiss and Kristin Archick, U.S.-EU Data Privacy: From Safe Harbor to Privacy Shield, Congressional Research Service, May 19 2016.

[1046] Case T-670/16 *Digital Rights Ireland v Commission* 16 September 2016

[1047] Case T-378/16 *La Quadrature du Net and Others v Commission* 25 October 2016

[1048] *Roman Zakharov v Russia*, Application no. 47143/06, (ECtHR, 4 December 2015)

surveillance.[1049] Here, the ECtHR determined that the secret mobile phone interception regime in Russia violated ECHR Art 8. However, the court went further and underlined that the very existence of such a surveillance system could lead to a citizen claiming that their Art 8 rights had been violated. The ECtHR had dealt with a similar case before in *Klass* which was discussed in Chapter 4. Although no breach of Art 8 was found in *Klass*, it was in *Zakharov*. If this indicates the future direction of ECtHR rulings it presents a blow to mass Internet surveillance and may well be used against the UK's Investigatory Powers Act as Cannataci points out.[1050]

On 21 December 2016, the CJEU published a preliminary ruling in two joined cases. The cases were brought by the Swedish and the UK courts of appeal.[1051] The Swedish case refers to an order from the Swedish authorities to Tele2 Sverige AB, a Swedish CSP, requiring it to retain metadata. The UK case resulted from action brought by Davis *et al* which resulted in the disapplication of DRIPA s.1 and that was depicted in Chapter 4.[1052] The Court ruled that EU-wide legislation means that national laws cannot require the 'general and indiscriminate retention'[1053] of metadata. Furthermore, national laws cannot permit access to retained data unless such access is for the investigation of serious crime and the access has received judicial or independent review.[1054] The Court stressed its concerns that mass retention of data may give people the impression that they live under constant

---

[1049] Cannataci (n 1026) 36

[1050] Ibid., 38

[1051] *Joined cases C-203/15 and C-698/15, Tele2 Sverige AB v Post-och Telestyrelsen and Secretary of State for the Home Department v Tom Watson and others* (Grand Chamber, 21 December 2016)

[1052] Note that Davis is not listed as a respondent in C-698/15; he subsequently became the Secretary of State for Exiting the European Union.

[1053] Joined cases C-203/15 and C-698/15 (n 1137) 134(1)

[1054] Ibid., 134(2)

surveillance.[1055] This is a clear threat to personal autonomy and demonstrates the Court's willingness to tackle the serious issues surrounding mass Internet surveillance.

7.4.4 Is Internet privacy dead?

Kupfer (Section 2.2 page 18) tells us that privacy enables personal autonomy and enables us to determine what is known about us. Wacks (Section 2.2 page 21) defines personal information to be any information about us which we would reasonably wish to keep to ourselves and Westin (Section 2.2 page 21) defines the control of such information as informational privacy. Our autonomy to protect our deepest secrets and desires is in danger of being stripped away by mass Internet surveillance, striking at our very individuality.[1056] The mere existence of mass Internet surveillance programmes can lead to the public being constantly concerned that they are being surveiled.[1057] If one thinks that one is always under surveillance one may change one's whole routine. The totally invasive nature of mass Internet surveillance is the critical issue. For example, two people may choose to meet in a private room to ensure they are not eavesdropped upon, or may choose to meet in such a way as each person is unaware of the identity of the other, maintaining their anonymity. This represents a clear indication of their reasonable expectation of privacy. One may argue that the room might be bugged, but not *all rooms everywhere* will be bugged. In order to avoid the possibility of a room being bugged, these two people may go to some remote location away from civilisation. Mass Internet surveillance removes this possibility. Yet, it overlooks the fact that terrorists can and presumably do communicate with great care, choosing their locations carefully. Thus, mass Internet surveillance is a major threat to privacy and can never be consistent with personal autonomy.

[1055] Ibid., 100

[1056] Westin (n 42) 33-34

[1057] *Klass and Others v Germany* (n 535) 41

The four cases outlined above serve to illustrate that the courts will judge mass Internet surveillance critically. The IPT case and *Zakharov* were argued on the issues of accessibility and foreseeability whereas *Schrems* and *Tele2* were argued on necessity and proportionality. Although these cases were heard by the UK, Ireland, the CJEU and ECHR the criteria on which the cases were judged are all present in the ICCPR. As an International instrument this is the only one potentially fit to be used against the current global mass Internet surveillance regimes.

Terrorist attacks do, of course, focus the public's attention. One may consider that if MI5 had carried out far more intense and wider surveillance it may have discovered the plan to bomb London in 2007. However, had it done so, the sheer size of the surveillance operation required would have had 'huge ramifications for our society and the way we live.'[1058] Even with such a surveillance regime, as Anderson and Killock highlight, '[k]nowledgeable villains will continue to use Skype, encrypted Gmail, throwaway mobiles and whatever comes next.'[1059] The general concern for privacy is that while terrorists and criminals will use such techniques, Internet users in general whether they are innocent or otherwise will remain under surveillance. This is compounded by the fact that as technologies evolve, legislation written to cater for such changes have not been future-proof. At the end of the day, while terrorists may cause us to restrict our movements or revisit our personal security, mass Internet surveillance strips us of our fundamental right to privacy and all that it protects. There is a risk that the terrorist wins simply by existing and not through any other action.

Is Internet privacy dead? It is difficult to answer with a binary yes or no. If Internet privacy is dead, it has to be completely, and while there is still some

---

[1058] Intelligence and Security Committee, 'Could 7/7 Have Been Prevented?' Review of the Intelligence on the London Terrorist Attacks on 7 July 2005' (Cm 7617), p40

[1059] Ross Anderson and Jim Killock, The Foundation for Information Policy Research and the Open Rights Group: Consultation response on Interception Modernisation or 'Protecting the Public', 15 July 2009

hope, it cannot be. So, the simple answer is no, Internet privacy is not dead even though it may appear that it was. However, the situation remains in flux. It is hard to be optimistic for the future in the light of the 2013 Snowden revelations and ongoing changes to legislation, in particular the Investigatory Powers Act in the UK. As has been discussed above legislative measures – laws and regulations – are the only effective means by where Internet privacy can be recovered. Technical advances will continue to improve the functionality of the Internet and hardware and software manufacturers will continue to bring new products to market with encryption built in. These are not the issue. The issue is that with every advance the intelligence agencies will also advance their collection strategies to further promote and enable mass Internet surveillance. The UN must take up this challenge and critically examine the surveillance regimes in place, in particular in the US and the UK and report as to whether these meet the criteria set out in Section 7.3.3 above. The Special Rapporteur is in post and has plans in place to carry out such an investigation. As stated by the American Civil Liberties Union (ACLU) '[i]f anything is anathema to the purpose of Article 17, it is the wholesale and deliberate collection of personal data or metadata about millions of people under no suspicion whatsoever.'[1060]

7.5 Conclusion and further research

Internet privacy is not dead but is in grave danger. This research has explored the meaning of privacy and focused on Internet privacy in the face of mass Internet surveillance. It has produced an in-depth analysis of the Internet from a technical perspective in order to better illustrate the areas where privacy is most at risk. Solutions were proposed that can maintain Internet privacy in the face of ongoing mass Internet surveillance.

This research has found several areas ripe for further study. During the course of this research data protection took centre stage and had real effects on

---

[1060] American Civil Liberties Union, 'Informational Privacy in the Digital Age: A Proposal to Update General Comment 16 [Right to Privacy] to the International Covenant on Civil and Political Rights', February 2015

certain aspects of legislation. The fall of Safe Harbor and the potential fall of the replacement Privacy Shield is another area ripe for in-depth analysis.

Furthermore, with large players now setting up data centres in countries and forming country-specific cloud services where data remains within a given jurisdiction is a developing area. How this effects the mass Internet surveillance activities of the US and the UK remains to be seen.

The legal fighting over the Snowden revelations is set to continue. Cases brought to the ECtHR are yet to be heard. Three cases are waiting to progress through the Court. All three cases deal with the issues surrounding PRISM, Upstream and Tempora.[1061] Depending on the outcome these cases may well yet have a major impact on mass Internet surveillance in the UK.

Also, it is interesting to note that companies are now prepared to fight rather than simply turning data over. Microsoft and Apple were both named in the Snowden revelations as being involved in the PRISM program. In the post-Snowden world with the EU expressing concerns over the data of its citizens major players such as Microsoft creating country-specific cloud services governed by third parties may well be clever marketing but does offer actual protection from US mass Internet surveillance.

However, the political situation is still very much in flux. The US saw the end of the Obama administration and the beginning of the Trump administration on 20 January 2017, and the UK's plans to leave the EU should be confirmed in March 2017 when the government proposes to sign Art. 50 of the Lisbon Treaty. In addition to leaving the EU and thus the decisions of the CJEU, the Conservatives have stated before that while they agree in principle with the ECHR, the directions of the ECtHR and the HRA have 'eroded public

---

[1061] *Big Brother Watch and others against the United Kingdom*, lodged 4 September 2013, App. No. 58170/13; *Bureau of Investigative Journalism and Alice Ross against the United Kingdom*, lodged 11 September 2014, App. No. 62322/14; *10 Human Rights Organisations and others v United Kingdom*, App. No. 24960/15

confidence'[1062] in the UK's approach to human rights. It may well be that the UK of the future sets itself aside from the ECHR and decisions of the ECtHR, the CJEU, and the EU Charter of Fundamental Rights. In the US, the incoming administration already has a CIA director in favour of increasing surveillance[1063] and it has been reported as likely that the Justice department will be less aggressive when it comes to protecting civil rights.[1064] Given this, and the intrusive nature of the Investigatory Powers Act we may well yet find that Internet privacy in the US and the UK has finally met its match.

[1062] Conservatives, Protecting Human Rights in the UK: the Conservatives' proposal for Changing Britain's Human Rights Laws, <https://www.conservatives.com/~/media/files/downloadable%20files/human_rights.pdf> accessed 20 January 2017

[1063] Kaveh Waddell, 'Trump's CIA Director Wants to Return to a Pre-Snowden World', (*The Atlantic* 18 November 2016) <http://www.theatlantic.com/technology/archive/2016/11/trumps-cia-director-wants-to-return-to-a-pre-snowden-world/508136/> accessed 28 December 2016

[1064] Matt Zapotosky, Wesley Lowery and Mark Berman, 'President Trump's Justice Dept. could see less scrutiny of police, more surveillance of Muslims', (*Washington Post*, 10 November 2016) <https://www.washingtonpost.com/world/national-security/donald-trump-preached-law-and-order-now-likely-comes-less-police-scrutiny-more-surveillance-of-muslims/2016/11/10/c430a234-a696-11e6-ba59-a7d93165c6d4_story.html?utm_term=.e209a7e9cefb> accessed 28 December 2016

Bibliography

—— ‘Barack Obama defends US surveillance tactics’ (*BBC*, 8 June 2013) <http://www.bbc.co.uk/news/world-us-canada-22820711>

—— ‘Britain’s GCHQ Hacked Belgian Telecoms Firm’ (*Spiegel Online*, 20 September 2013) <http://www.spiegel.de/international/europe/british-spy-agency-gchq-hacked-belgian-telecoms-firm-a-923406.html>

—— BULLRUN (undated) <https://search.edwardsnowden.com/docs/BULLRUN2014-12-28nsadocs>

—— BULLRUN CoI briefing sheet (undated) <https://search.edwardsnowden.com/docs/BULLRUNCoI–BriefingSheet2013-09-05nsadocs>

—— China Media Bulletin, issue 5 January 13 2011, ‘Chinese government expands mobile-phone controls’

—— ‘Deep Dive into Quantum Insert’ (*Fox IT*, 20 April 2015) <https://blog.fox-it.com/2015/04/20/deep-dive-into-quantum-insert/>

—— GCHQ Network Analysis Centre, Mobile Networks in MyNOC World, slide 9 <https://search.edwardsnowden.com/docs/MobileNetworksinMyNOCWorld2014-12-13nsadocs>

—— Microsoft releases new service, affects FAA702 collection <https://search.edwardsnowden.com/docs/MicrosoftreleasesnewserviceaffectsFAA702collection2014-05-13nsadocs>

—— NIST Removes Cryptography Algorithm from Random Number Generator Recommendations, 21/04/14 <http://www.nist.gov/itl/csd/sp800-90-042114.cfm>

—— Speech by Bill Clinton at the Paul H. Nitze School of Advanced International Studies, Washington D.C., Mach 8, 2000 <http://usinfo.org/wf-archive/2000/000380/epf302.htm>

—— ‘Spy law used in dog fouling war’ (*BBC News*, 27 April 2008) <http://news.bbc.co.uk/1/hi/uk/7369543.stm>

—— Tor Stinks, June 2012 <https://search.edwardsnowden.com/docs/TorStinks2013-10-04nsadocs>

35th International Conference of Data Protection and Privacy Commissioners, Resolution on anchoring data protection and the protection

of privacy in international law <https://icdppc.org/wp-content/uploads/2015/02/International-law-resolution.pdf>

40 Weekly Compilation of Presidential Documents 641, April 20 2004 <http://www.gpo.gov/fdsys/pkg/WCPD-2004-04-26/pdf/WCPD-2004-04-26-Pg638.pdf>

Adrian D and others, Imperfect Forward Secrecy: How Diffe-Hellman Fails in Practice, CCS'15 The 22nd ACM Conference on Computer and Communications Security, 12-16 October 2-15 <https://weakdh.org/imperfect-forward-secrecy-ccs15.pdf>

Akdeniz Y, Walker C and Wall D, *The Internet: law and society* (Pearson, Harlow, 2000)

Akhawe D and Porter Felt A, 'Alice in Warningland: A large-scale field study of browser security warning effectiveness', Proceedings of the 22nd USeNIX Security Symposium, August 14-16 2013, Washington D.C., s.8 <https://www.usenix.org/sites/default/files/sec13-proceedings.epub>

Aldrich R J, *GCHQ: the uncensored story of Britain's most secret intelligence agency* (Harper Press, London, 2010)

All Party Parliamentary Communications Group ' "Can we keep our hands off the net?" Report of an Inquiry by the All Party Parliamentary Communications Group', October 2009

American Civil Liberties Union, 'Informational Privacy in the Digital Age: A Proposal to Update General Comment 16 [Right to Privacy] to the International Covenant on Civil and Political Rights', February 2015

Amesys, From Lawful to Massive Interception: Aggregation of sources, <https://wikileaks.org/spyfiles/files/0/21_200810-ISS-PRG-AMESYS.pdf>

Amesys Intelligence Solutions <https://wikileaks.org/spyfiles/document/amesys/95_critical-system-architect/95_critical-system-architect.pdf>

Amnesty International, People's Republic of China: controls tighten as Internet activism grows, (Amnesty International, 2004, ASA 17/001/2004)

—— People's Republic of China: state control of the Internet in China, (Amnesty International, 2002, ASA 17/007/2002)

Anderson R and Killock J, The Foundation for Information Policy Research and the Open Rights Group: Consultation response on Interception Modernisation or 'Protecting the Public', 15 July 2009

Article 29 Data Protection Working Party, Opinion 4/2005 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)438 final of 21.09.2005), WP 113

—— Opinion 5/2002 on the Statement of the European Data Protection Commissioners at the International Conference in Cardiff (9-11 September 2002) on mandatory systematic retention of telecommunication traffic data, 11818/02/EN/Final, WP 64, 11 October 2002

Barnum D, 'Warrantless electronic surveillance in national security cases: lessons from America', E.H.R.L.R 514, 2006

Basu S and others, Open letter from UK internet law academics, <http://www.law.ed.ac.uk/__data/assets/pdf_file/0003/158070/Open_letter_UK_internet_law_academics.pdf>

Bellia P L, 'The "Lone Wolf" Amendment and the Future of Foreign Intelligence Surveillance Law', 50 Vill. L. Rev. 425 2005

Bergen P and others, Do NSA's bulk surveillance programs stop terrorists?, New America Foundation, January 2014, p4 <https://static.newamerica.org/attachments/1311-do-nsas-bulk-surveillance-programs-stop-terrorists/IS_NSA_surveillance.pdf>

Bernstein D, Tanja Lange and Ruben Niederhagen, Dual EC: A Standardized Back Door, p2 <https://projectbullrun.org/dual-ec/documents/dual-ec-20150731.pdf>

Besson S, 'The reception process in Ireland and the United Kingdom' in Helen Keller and Alec Stone Sweet (eds) *A Europe of rights: the impact of the ECHR on national legal systems*, (OUP, Oxford, 2008)

BeVier L R 'The Communications Assistance for Law Enforcement Act of 1994: a surprising sequel to the break up of AT&T' 51 Stanford L. Rev. 1049

Bilge L and Dumitras T, 'Before We Knew It: an Empirical Study of Zero-Day Attacks In The Real World', CCS '12: Proceedings of the 2012 ACM Conference on Computer and Communications Security, October 2012.

Birkenstock G, 'The Foreign Intelligence Surveillance Act and standards of probable cause: an alternative analysis', 80 Georgetown L. Rev. 843 (1992)

Blaze M, Protocol Failure in the Escrowed Encryption Standard, 20 August 1994 <http://www.crypto.com/papers/eesproto.pdf>

Braden R, ‘Requirements for Internet Hosts – Communication Layers’, RFC1122, <http://tools.ietf.org/html/rfc1122>

Bradley A A, ‘Extremism in the defense of liberty?: the Foreign Intelligence Surveillance Act and the significance of the USA PATRIOT Act’, 77 Tul. L. Rev. 465 2002-2003

Bright P, ‘Microsoft to offer UK–based Azure, Office 365 from late 2016’ (*Arstechnica*, 11 November 2015) <http://arstechnica.co.uk/information-technology/2015/11/microsoft-to-offer-uk-based-azure-office-365-from-late-2016>

Brin D, *The transparent society* (Basic Books, New York, 1998)

Brown I, Regulation of converged communications surveillance, SSRN id 1261192, 2009

Brown I and Korff D, ‘Terrorism and the Proportionality of Internet Surveillance’, European Journal of Criminology 6(2), 2009

Buckley S, ‘Windstream establishes 100G express route in red-hot Ashburn, Va. Market via NJFX’, (*FierceTelecom*, 19 January 2016) <http://www.fiercetelecom.com/telecom/windstream-establishes-100g-express-route-red-hot-ashburn-va-market-via-njfx>

Butler K and others, ‘A Survey of BGP Security Issues and Solutions’, 98 Proc. IEEE 1, January 2010

Cady S S, ‘Reconciling privacy with progress: Fourth Amendment protection of e-mail stored with and sent through a third-party Internet service provider’, 61 Drake L. Rev. 225 2012-2013

Callanan C, and others, Leaping over the Firewall: a review of censorship circumvention tools, Freedom House

Cannataci J, Report of the Special Rapporteur on the right to privacy, UN Human Rights Council, A/HRC/31/64, 24 November 2016

Cao J, 'Protecting the right to privacy in China', 36 Victoria U. Wellington L. Rev. 645

Cardy E A, ‘The Unconstitutionality of the Protect America Act of 2007’, 18 B.U. Pub. Int. L. J.171 2008-2009

Casey T, ‘Electronic surveillance and the right to be secure’, 41 UC Davis L R 3, 2008

Cate F H, ‘Government Data Mining: The Need for a Legal Framework’, 43 Harv. C.R.-C.L. L. Rev. 435, 2008

Cavoukian A, International Council on Global Privacy & Security by Design, <http://gpsbydesign.org>

CCPR General Comment No.16: Article 17 (Right to privacy) The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation, Adopted at the Thirty-second Session of the Human Rights Council, on 8 April 1988, 4

Chadwick P, 'The value of privacy', EHRLR 2006, 5, 495-508

Charlesworth A, ‘Information Privacy Law in the European Union: E Pluribus Unum or Ex Uno Plures?’, 54 Hastings L. J. 931 2002-2003

Chen W, Concerning the development and administration of our country's Internet, (HRIC tr.) I (3) <http://www.hrichina.org/crf/article/3242>

Cheung A S Y, China Internet going wild: Cyber-hunting versus privacy, Comp. L. & Security Rev. 25 (2009) 275-279

China Media Bulletin, issue 6 January 20 2011, ‘Stand-alone cybercafes to be eliminated in China by 2016’

CIW Team, WeChat monthly active users reached 806 million in Q2 2016 <https://www.chinainternetwatch.com/18789/wechat-monthly-active-users-reached-806-million-in-q2-2016/>

—— Weibo Search Users Insight 2015 <https://www.chinainternetwatch.com/16366/weibo-search-users-insights-2015/>

Clegg N, The surveillance bill is flawed but at least we have oversight, The Guardian, 5/Nov/15 <http://www.theguardian.com/commentisfree/2015/nov/05/surveillance-bill-mi5-secret-database>

Comer D E, *Interworking with TCP/IP: Volume 1; principles, protocols and architecture* (Prentice-Hall, US, 1991)

Conservatives, Protecting Human Rights in the UK: the Conservatives’ proposal for Changing Britain’s Human Rights Laws, <https://www.conservatives.com/~/media/files/downloadable%20files/human_rights.pdf>

Cooley T, *A treatise on the law of torts or the wrongs which arise independent of contract* (Callaghan and Co., Chicago, 1880)

Cooper Blum S, ‘What really is at stake with the FISA Amendments Act of 2008 and ideas for future surveillance reform’, 18 B.U. Pub. Int. L. J. 269 2008-2009

Cousens M, *Surveillance Law* (Reed Elsevier, 2004)

Cullen R and Choy P D W, ‘The Internet in China’, 13 Colum. J. Asian L. 99 1999

D’Jaen M D, Breaching the Great Firewall of China: Congress Overreaches in Attacking Chinese Internet Censorship, 31 Seattle U. L. Rev. 327 2007-2008

Determann L and Sprague R, ‘Intrusive monitoring: employee privacy, expectations are reasonable in Europe, destroyed in the United States’, 26 Berkeley Tech. L.J. 979 2011

Diffie W and Landau S, *Privacy on the Line: The Politics of Wiretapping and Encryption* (MIT Press, Cambridge, 1998)

DiLascio T, ‘How safe is the Safe Harbor? U.S. and E.U. data privacy law and the enforcement of the FTC’s Safe Harbor Program’, 22 B.U. Int’l L.J. 399 2004

Dingledine R, Mathewson N and Syverson P, Tor: the second-generation onion router, Proc. Of the 13th Usenix security symposium, August 2004, 303-320

Dobinson I and Johns F, ‘Qualitative Legal Research’ in McConville M and Chiu W H (Eds.) *Research Methods for Law* (Edinburgh University Press, Edinburgh, 2007),

Donley C and others, ‘Assessing the impact of NAT444 on network applications, Internet Engineering Task Force’, 25 October 2010 <http://tools.ietf.org/html/draft-donley-nat444-impacts-01>

Donnelly R C, ‘Electronic Eavesdropping’, 38 Notre Dame L. 667 1962-1963

Eastlake D, ‘Transport Layer Security (TLS) Extensions: Extension Definitions’, RFC6066 <https://tools.ietf.org/html/rfc6066>

Electronic Privacy Information Center, *Privacy & Human Rights: an international survey of privacy laws and developments* (Electronic Privacy Information Center, 2003)

Emmerson B, Promotion and protection of human rights and fundamental freedoms while countering terrorism, UN General Assembly, A/69/397, 23 September 2014

Emmott R, ‘Brazil, Europe plan undersea cable to skirt U.S. spying’ (*Reuters*, 24 February 2014) <http://www.reuters.com/article/us-eu-brazil-idUSBREA1N0PL20140224>

Eskens S, van Daalen O and van Eijk N, ’10 Standards or Oversight and Transparency of National Intelligence Services’, 8 J. Nat’l Sec. L. & Pol’y 553 2015-2016

Etzioni A, ‘The Privacy Merchants: What Is To Be Done?’, 14 U. Pa. J. Const. L. 929, 952 (2012)

Fallows J, ‘The connection has been reset’ (*The Atlantic*, March 2008) <http://www.theatlantic.com/magazine/archive/2008/03/the-connection-has-been-reset/306650/>

Farrell S and Tschofenig H, Pervasive Monitoring is an Attack <https://tools.ietf.org/html/rfc7258>

Farris R, Roberts H and Wang S, ‘China’s Green Dam: the implications of government control encroaching on the home PC’, (OpenNet Initiative Bulletin, undated)

Federal Government Information Technology: Electronic Surveillance and Civil Liberties (Washington CD, US Congress, Office of Technology Assessment, OTA-CIT-293, October, 1985) <http://www.justice.gov/sites/default/files/jmd/legacy/2013/10/15/fgit-1985.pdf>

Feldman D, *Civil liberties and human rights in England and Wales*, (2nd edn) (OUP, Oxford, 2002)

—— 'Human dignity as a legal value: part 1', [1999] Public Law 682

—— 'Privacy-related rights and their social value', in Birks, P., (ed) *Privacy and Loyalty* (Clarendon, Oxford, 1997)

Fisher L, ‘Congress and the fourth amendment’, 21 Ga. L. Rev. 107 1986-1987

Fung E S K, 'The idea of freedom in modern China revisited: plural conceptions and dual responsibilities', Modern China, Vol. 32, No. 4 (Oct 2006) 453

Gannon J, ‘From Executive Order to Judicial Approval: Tracing the History of Surveillance of U.S. Persons Abroad in Light of Recent Terrorism Investigations’, 6 J. Nat’l Sec. L. & Pol’y 59 2012

Greenleaf G, *Asian Data Privacy Laws: Trade and Human Rights Perspectives* (OUP, 2014)

Gorkin R, ‘The constitutional right to information privacy: NASA v. Nelson’, 6 Duke J. of Constitutional Law & Public Policy Sidebar

Gou Z and Wu M, ‘Dancing thumbs: Mobile telephony in contemporary China’, in Zhang X and Zheng Y, (Eds.) *China’s Information and Communications Technology Revolution: Social changes and state responses* (Routledge, Abingdon 2009)

Grimmelmann J, ‘Facebook and the Social Dynamics of Privacy’ (New York Law School Legal Studies, Research paper series 08/09 #7)

Hachigian N, ‘China’s Cyber–Strategy’, 80 Foreign Aff. 118 2001

Haggerty K D and Samatas M, ‘Surveillance and democracy: an unsettled relationship’ in Haggerty K D and Samatas M (eds.) *Surveillance and Democracy* (Routledge-Cavendish, Oxon, 2010)

HC Deb 08 March 1979 vol 963

HC Deb 01 April 1980 vol 982 cc205-220

HC Deb 01 April 1981 vol 2 cc321-72

HC Deb 12 March 1985 vol 75 cc151-241

HC Deb 06 March 2000 vol 345 cc767-835

HC Oral Answers 4 Nov 2015

HL Deb 19 March 1984 vol 449 cc977-1036

Herold D K, ‘An inter-nation-al Internet: China’s contribution to global Internet governance?’ <http://ssrn.com/abstract=1922725>

Hindocha N and Chien E, ‘Malicious Threats and Vulnerabilities in Instant Messaging, Symantec Security Response White Paper, 2003’ <https://www.symantec.com/avcenter/reference/malicious.threats.instant.messaging.pdf>

Hirshleifer J, 'Privacy: its origin, function, and future', 9 J Legal Studies 4 649-664 (Dec 1980)

Hobby S P, ‘The EU Data Protection Directive: Implementing a Woldwide Data Protection Regime and How the U.S. Position has Progressed’, 1 Int’l L. & Mgmt. Rev. 155 2005

Hodgson G, ‘Breaking Encryption and Gathering Data: International Law Applications’, 20 J. Tech. L. & Pol’y 39, 2015

Home Office, Communications Data Draft Code of Practice, August, 2016 <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/557862/IP_Bill_-_Draft_CD_code_of_practice.pdf>

—— *Draft Structural Reform Plan*, July 2010

—— *Interception of Communications in the United Kingdom: a consultation paper* (Cm. 4368, June 1999)

—— *Interception of Communications Code of Practice Pursuant to section 71 of the Regulation of Investigatory Powers Act 2000*

—— *Protecting the Public in a Changing Communications Environment* (Cm 7586, 2009)

—— *Report of the Committee on Data Protection* (Cmnd. 7341, 1978)

—— *Report of the Committee on Privacy* (Cmnd. 5012, 1972)

—— *Report of the Committee on Privacy and Related Matters* (Cm 1102, 1990)

—— *The Interception of Communications in Great Britain* (Cmnd. 7873, 1980)

Hoogstraaten H and others, ‘Black Tulip: report of the investigation into the DigiNotar Certificate Authority breach’ (Fox-IT BV, Delft, 2012), p3 <https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/rapporten/2012/08/13/black-tulip-update/black-tulip-update.pdf>

Horn K A, ‘Privacy versus protection: exploring the boundaries of electronic surveillance in the Internet age’, 29 Fordham Urb. L. J. 2001-2002

House of Commons Science and Technology Committee, Investigatory Powers Bill: technology issues, Third report of Session 2015-16, HC 573

House of Lords Select Committee on Science and Technology 5th Report, 1996, HL 77

House of Lords, House of Commons, *Joint Committee on Draft Communications Data Bill, session 2012-13, written evidence*

—— *Joint Committee on the Draft Investigatory Powers Bill report*, HL Paper 93, HC 651, 3/2/16

Hurwitz J, ‘Trust and online interaction’, 161 U. Pa. L. Rev. 1579

Hutchinson T and Duncan N, ‘Defining and Describing What We Do: Doctrinal Legal Research’, 17 Deakin L. Rev. 83 (2017)

Information Office of the State Council of the People’s Republic of China: National Human Rights Action Plan of China (2009-2010)

—— National Human Rights Action Plan of China (2012-2015)

Intelligence and Security Committee, ‘Could 7/7 Have Been Prevented?’ Review of the Intelligence on the London Terrorist Attacks on 7 July 2005’ (Cm 7617)

Intelligence and Security Committee of Parliament, ‘Statement on GCHQ’s Alleged Interception of Communications under the US PRISM Programme’ <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/225459/ISC-Statement-on-GCHQ.pdf>

International Centre for Human Rights and Democratic Development, Review of China’s Internet Regulations and Domestic Legislation

International Telecommunications Union, ‘ICT Facts and Figures 2016’ <https://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2016.pdf>

—— ‘Key ICT indicators for developed and developing countries and the world (totals and penetration rates)’ http://www.itu.int/en/ITU-D/Statistics/Documents/statistics/2016/ITU_Key_2005-2016_ICT_data.xls

Investigatory Powers Tribunal report 2011-2015 <http://ipt-uk.com/docs/IPT%20Report%202011%20-%202015.pdf>

Joergensen R F, 'Security and Privacy in Cyberspace' in Stauffacher D and Kleinwächter W, (eds) *The World Summit on the Information Society: Moving from the Past into the Future* (UN ICT Task Force, 2005)

Justice, Protecting the Public in a Changing Communications Environment: JUSTICE Response to the Home Office Consultation, July 2009

Kaye D, ‘State Execution of the International Covenant on Civil and Political Rights’, 3 UC Irvine L. Rev. 95

Keeton W P (ed), *Prosser and Keeton on Torts* (5th edn) (West, Minnesotta, 1984)

Kelly S, 'The spread of our digital footprint' <http://news.bbc.co.uk/1/hi/programmes/click_online/7380645.stm>

Kelly S and Cook S, ‘New Technologies, Innovative Repression: Growing Threats to Internet Freedom’ in Sanja Kelly and Sarah Cook (Eds.) *Freedom on the Net 2011: A Global Assessment of Internet and Digital Media*, (Freedom House, 2011)

Kerr O, ‘A user's guide to the Stored Communications Act, and a legislator's guide to amending it’, 72 Geo. Wash. L.Rev 1208 2003-2008

—— The Volokh Conspiracy archive, 17/04/07 <www.volokh.com/posts/1176832897.shtml>

—— The Volokh Conspiracy archive, 18/06/07 <www.volokh.com/posts/1182181742.shtml>

Kissel T K, ‘License to Blog: Internet Regulation in the People’s Republic of China’, 17 Ind. Int’l & Comp. L. Rev. 229 2007

Klein M, *Wiring up the big brother machine… and fighting it* (Booksurge, South Carolina, 2009)

Knoll A, ‘Any which way but loose: nations regulate the Internet’, 4 Tul. J. Int’l & Comp. L. 275 1995-1996

Kraus R, ‘Statistical Dèjá Vu: The National Data Center Proposal of 1965 and Its Descendants’ 5 J. Privacy & Confidentiality 1 (2013) 1-37

Kupfer J, 'Privacy, autonomy and self-concept', 24 American Philosophical Quarterly 1 (Jan 1987)

LaFave W R, Jerold H Israel and Nancy J King, *Criminal Procedure (3rd edn.)* (West Group, Minnesota, 2000)

Landau S, Making sense from Snowden: what’s significant in the NSA surveillance revelations, IEEE Security and Privacy, July/August 2013

—— ‘National security on the line’, 4 J. Telecomm. & High Tech. L. 409 2005-2008

—— *Surveillance or Security? The Risks Posed by New Wiretapping Technologies* (The MIT Press, Cambridge, 2010)

Lee J-A and Liu C-Y, Real-name registration rules and the fading digital anonymity in China, 25 Pac. Rim L. & Pol’y J. 1, 2016

Lessig L, ‘The Architecture of Privacy’, 1 Vand. J. Ent. L. & Prac. 56 1999

—— *Code version 2.0*, (Basic Books, New York, 2006)

Li C, ‘Internet Content Control in China’, 8 Int’l J. Comm. L. & Pol’y. 1

Li Y and Otto J M, ‘Central and Local Law-Making: Studying China’s Experience’, in Vermeer E and d’Hooghe I (eds) *China’s Legal Reforms and Their Political Limits* (Curzon, Richmond, 2002)

Liang G and Huili C, Surveillance and privacy in urban China, the Globalization of Personal Data project, Queen's University, 2006

Ling G F, *China developing: cultural identity of emerging societies* (World Scientific, Singapore, 2008)

Littman M and Carter-Ruck P ‘Privacy and the Law, a report by Justice’, 1970

Lloyd I J, ‘The Interception of Communications Act 1985’, 49 MLR January 1986 86-95

LSE, Briefing on the Interception Modernisation Programme, PEN paper 5

MacAskill E and others, ‘GCHQ taps fibre-optic cables for secret access to world’s communications’, (*The Guardian*, 21/June/2013) <http://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa>

Maclin T, ‘The Bush administration’s terrorist surveillance program and the Fourth Amendment’s warrant requirement: lessons from Justice Powell and the *Keith* case’, 41 U.C. Davis L. Rev. 1262 2007-2008

McCoy D and others, ‘Shining light in dark places: understanding the Tor network’, in Nikita Borisov and Ian Goldberg, (eds.) *Privacy enhancing technologies, Proc. 8th international symposium, PETS 2008, Leuven, Belgium, July 2008* (Springer, Berlin, 2008)

McDougall B S, 'Particulars and universals: studies on Chinese privacy' in McDougal B S and Hansson A (eds) *Chinese Concepts of privacy* (Brill, The Netherlands, 2002)

McIntosh M K, *Controlling misbehaviour in England, 1370 – 1600* (Cambridge University Press, Cambridge, 1998)

McIntyre J, ‘Balancing expectations of online privacy: why Internet Protocol (IP) addresses should be protected as personally identifiable information’, 60 DePaul L. Rev. 895 2010-2011

Margaret M, Coming of Age in Samoa (Penguin, Middlesex, 1943)

Meason J E, ‘The Foreign Intelligence Surveillance Act: time for reappraisal?’, 24 Int'l L 1043 (1990)

Menn J, ‘Exclusive: Secret contract tied to NSA and security industry pioneer’, (*Reuters*, 20 December 2013) <http://www.reuters.com/article/2013/12/20/us-usa-secuity-rsa-idUSBRE9BJ1C220131220>

Microsoft Cloud Germany <http://download.microsoft.com/download/6/1/3/613C9ECB-9167-4EF5-B131-3BAD8D8A126C/Microsoft_Cloud_Germany_Datasheet.pdf>

Mikaelsen L, *European protection of human rights*, (Sijthoff & Noordhoff, The Netherlands, 1980)

Mindle M, 'Liberalism, Privacy and Autonomy', 51 J. Politics 1989 575

Miniwatts Marketing Group, ‘Internet in Europe Stats’ <http://www.internetworldstats.com/stats4.htm#europe>

—— ‘Internet Usage and 2015 Population in North America’ <http://www.internetworldstats.com/stats14.htm#north>

—— ‘Internet Usage in Asia’ <http://www.internetworldstats.com/stats3.htm#asia>

Moore A D, ‘Privacy’ in Hugh LaFollette (ed.) *International Encyclopedia of Ethics* (Wiley, Chichester, 2013)

Narten T, Draves R and Krishnan S, Privacy extensions for stateless address autoconfiguration in IPv6, September 2007, RFC4941 <https://tools.ietf.org/html/rfc4941>

Neal D, ‘AES Encryption is cracked’ (*the Inquirer*, 17 August 2011) <http://www.theinquirer.net/inquirer/news/2102435/aes-encryption-cracked>

Neiland A E, ‘National Security Letters and the amended Patriot Act’, 92 Cornell L. Rev. 1201 2006-2007

Nichols S, ‘Como-D’oh! Infosec duo exploits OCR flaw to nab a website’s HTTPS cert’, (*The Register*, 21 October 2016) <http://www.theregister.co.uk/2016/10/21/comodoh_researchers_exploit_image_recognition_bug_to_steal_certs/>

Nordrum A, Quantum Computer Comes Closer to Cracking RSA Encryption, IEEE Spectrum, 3 march 2016 <http://spectrum.ieee.org/tech-talk/computing/hardware/encryptionbusting-quantum-computer-practices-factoring-in-scalable-fiveatom-experiment>

Nowak M, *UN covenant on civil and political rights: CCPR commentary* (Kehl, Germany, 2005, 2nd edn)

OED Online

Office of Inspectors General, Report on the President's Surveillance Program, Volume 1, 10 July 2009 <https://oig.justice.gov/reports/2015/PSP-09-18-15-vol-I.pdf>

Ong R, 'Recognition of the right to privacy on the Internet in China', 1 International Data Privacy Law 3, 2011

Office of the High Commissioner for Human Rights, The right to privacy in the digital age, A/HRC/27/37, 30 June 2014

Office of the Surveillance Commissioners Annual Report for 2009-2010

OpenNet Initiative, *Internet filtering in China in 2004-2005: A Country Study*

Oxford American Dictionary of Current English (OUP, Oxford, 1999)

Oxford Dictionary of Law, (OUP, Oxford, 2006, 6th edn)

Palfrey J, 'The public and the private at the United States border with cyberspace', 78 Miss. L.J. 242 2088-2009

Parent W A, 'Recent work on the concept of privacy', 20 American Philosophical Quarterly 4

Park G D, 'Internet wiretaps: applying the Communications Assistance for Law Enforcement Act to broadband services', 2 ISJLP 5990 2005-2006

Parker Voors M, 'Encryption regulation in the wake of September 11, 2001: must we protect national security at the expense of the economy?', 55 Fed. Comm. L.J. 331 2002-2003

Peng S Y, 'Privacy and the construction of legal meaning in Taiwan', 37 Int'l L. 1037 2003

Perry C, 'U.S. v Warshak: will Fourth Amendment protection be delivered to your inbox?', 12 N.C. J.L. & Tech. 345 2010-2011

Pew Internet and American Life Project, 'Digital Footprints: online identity management and search in the age of transparency', December 2007, <http://www.pewinternet.org>

Privacy and Civil liberties Oversight Board, Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act, July 2, 2014

—— Report on the Telephone Record Program Conducted under Section 215 of the USA PATRIOT Act and on the Operations of the Foreign Intelligence Surveillance Court, 23 January 2014, <https://fas.org/irp/offdocs/pclob-215.pdf>

Poulsen K, 'FBI admits is controlled Tor servers behind mass malware attack', (*Wired*, 13 September 2013) <https://www.wired.com/2013/09/freedom-hosting-fbi/>

Privy Council, *Report of the Committee of Privy Councillors appointed to inquire into the interception of communications* (Cmnd 283, October 1957)

Prosser W L, 'Privacy' 48 Cal. L. Rev 383 (1960)

Putnam B H, *Proceedings before the justices of the peace in the fourteenth and fifteenth centuries, Edward III to Richard III*, (Spottiswoode, London, 1938)

Qui Q, 'Personal data scam, 8 jailed' (*China Daily*, 01/05/2010) <http://www.chinadaily.com.cn/cndy/2010-01/05/content_9263566.htm>

Rauhofer J and Síthigh D M, 'The Data Retention Directive Never Existed', Scr*ip*t*ed* Volume 11, issue 1, April 2014

Reid A S and Ryder N, 'For whose eyes only? A critique of the United Kingdom's Regulation of Investigatory Powers Act 2000', Information & Communications Technology Law, 10:2, 179-201

Republican presidential candidates debate in Phoenix, Arizona, December 6th 1999 <http://www.presidency.ucsb.edu/ws/index.php?pid=75089>

Risen J and Lichtblau E, 'Bush lets U.S. spy on callers without courts', (*New York Times*, 16 December 2005) <http://www.nytimes.com/2005/12/16/politics/16program.html>

Robinson D, 'Amazon Web Services to open first UK data centre post Safe Harbour ruling' (*V3*, 6 November 2015) <http://www.v3.co.uk/v3-uk/news/2433779/amazon-web-services-to-open-first-uk-data-centre-post-safe-harbour-ruling>

Robinson G H, 'We're listening! Electronic eavesdropping, FISA, and the secret court', 36 Willamette L.Rev. 51 2000

Rotenberg M, 'Privacy and Secrecy after September 11', 86 Minn. L. Rev. 1115 2001-2002

Schneier B, Data mining for terrorists, 09/03/06 <https://www.schneier.com/blog/archives/2006/03/data_mining_for.htm>

Schoeman F D, *Privacy and Social Freedom*, (Cambridge University Press, 1992)

Science and Technology Committee (Commons), Investigatory Powers Bill: technology issues <http://www.publications.parliament.uk/pa/cm201516/cmselect/cmsctech/573/57305.htm>

Seipp D J, 'English judicial recognition of a right to privacy', 3 Oxford J Legal Studies 3 325

Senseney H A, 'Interpreting the Communications Assistance for Law Enforcement Act of 1994: the Justice Department versus the Telecommunications industry & privacy rights advocates'(1998) 20 Hastings Comm/Ent L.J. 665

Shaffer G, 'Globalization and Social Protection: The Impact of EU and international Rules in the Ratcheting Up of U.S. Privacy Standards', 25 Yale J. Int'l L. 1 2000

Shao G, *Internet law in China* (Chandos, Oxford, 2012)

Shattuck J, *Rights of privacy* (National Textbook Company, Illinois, 1977)

Shelton M and others, Pew Research Center, Americans' Privacy Strategies Post-Snowden, 16 March 2015 <http://www.pewinternet.org/files/2015/03/PI_AmericansPrivacyStrategies_0316151.pdf>

Shie T R, The Tangled Web: does the Internet offer promise or peril for the Chinese Communist Party?, J Contemporary China (2004)

Shumate B A, 'Thou shalt not speak: the nondisclosure provisions of the National Security Letter statutes and the First Amendment challenge', 41 Gonz. L. Rev 151 2005-2006

Sidhu D S, 'The chilling effect of government surveillance programs on the use of the Internet by Muslim-Americans' [2007] 7 U Maryland Journal of Race, Religion, Gender and Class

Singhal A K and Malik I, 'Doctrinal and socio-legal methods of research: merits and demerits', 2(7) Educational Research Journal 252-256

Sklansky D, 'Back to the future: *Kyllo*, *Katz* and common law', 72 Miss. L. J. 143 2002-2003

Snowden E (*Twitter*, 17 November 2016) <https://twitter.com/i/web/status/799371508808302596>

Solove D, ‘Reconstructing electronic surveillance law’ 72 Geo. Wash. L. Rev. 1264 (2003-2004)

—— The origins and growth of information privacy law, 20 <http://ssrn.com/abstract=445181>

—— *The digital person: technology and privacy in the Information Age*, (New York University Press, New York, 2004)

SSO Highlight - Microsoft Skydrive Now Part of PRISM Standard Stored Communication Collection <https://search.edwardsnowden.com/docs/SSOHIGHLIGHT–MicrosoftSkydriveCollectionNowPartofPRISMStandardStoredCommunicationsCollection2014-05-13nsadocs>

Tailored Access Operations, ‘Peeling Back the Layers of Tor with Egotistigal Giraffe’, <https://www.eff.org/files/2014/04/09/20131004-guard-egotistical_giraffe.pdf>

Taylor G, 'Privacy and the public' 34 MLR 3 (May 1971) 288-304

Taylor N W, ‘Policing, privacy and proportionality’, EHRLR 2003, Supp (special issue: privacy 2003)

The 9/11 Commission Report pp4-14

The Coalition: our programme for government, May 2010

The Enemies of the Internet: special edition : surveillance – China <http://surveillance.rsf.org/en/china/>

The Information Commissioner's response to "Protecting the Public in a Changing Communications Environment", 15 July 2009

The Royal Commission on Criminal Procedure (Cmnd 8092, January 1981)

Thompson J J, 'The Right to Privacy', Philosophy and Public Affairs, Vol 4, No 4 (Summer, 1975)

Torrieri D J, *Principles of secure communications systems (2nd edn.)* (Artech House, Boston, 1992)

Traver H, ‘Orientations toward privacy in Hong Kong’, Perception and Motor Skills 59(2), 1984, 635 – 644

Tugendhat M and Coppola A ‘Principles and Sources’ in Tugendhat M and Christie I, (eds) *The law of privacy and the media* (OUP, Oxford, 2002)

Tugendhat M, Nicklin M and Busuttil G, ‘Publication of Personal Information’ in Tugendhat M and Christie I, (eds) *The law of privacy and the media* (OUP, Oxford, 2002)

Tygar D D, 'Technological dimensions of privacy in Asia', 10 Asia-Pacific Review 2

UN Fact Sheet No.2 (Rev. 1) the International Bill of Human Rights, available from <http://www.ohchr.org/Documents/Publications/FactSheet2Rev.1.en.pdf> accessed 23 June 2010

United Nations General Assembly, Resolution adopted by the General Assembly on 18 December 2013, 68/167, The right to privacy in the digital age

United States Senate, *Final Report of the Select Committee to Study Governmental Operations with respect to Intelligence Activities: Book I: Foreign and Military Intelligence* (US Government Printing Office, Washington, 1976)

—— *Final Report of the Select Committee to Study Governmental Operations with respect to Intelligence Activities: Book II: Intelligence Activities and the Rights of Americans* (US Government Printing Office, Washington, 1976)

—— *Final Report of the Select Committee to Study Governmental Operations with respect to Intelligence Activities: Book III: Supplementary Detailed Staff Reports on Intelligence Activities and the Rights of Americans* (US Government Printing Office, Washington, 1976)

Villeneuve N, ‘Breaching trust: An analysis of surveillance and security practices on China’s TOM-Skype platform, Information Warfare Monitor / ONI Asia Joint Report’ <http://www.nartv.org/mirror/breachingtrust.pdf>

Viviane Reding, Letter to the US Attorney General from Viviane Reding, Vice-president of the European Commission, 10 June 2013, Ref. Ares (2013)193546

Wacks R, ‘The Poverty of Privacy’ (1980) 96 LQR 73

Waddell K, ‘Trump’s CIA Director Wants to Return to a Pre-Snowden World’, (*The Atlantic* 18 November 2016) <http://www.theatlantic.com/technology/archive/2016/11/trumps-cia-director-wants-to-return-to-a-pre-snowden-world/508136/>

Walker C, ‘Data retention in the UK: pragmatic and proportionate, or a step too far?’, Computer Law & Security Review, V25, issue 4, July 2009

Walker C and Akdeniz Y, ‘Anti-Terrorism Laws and Data Retention: War is Over?’, 54 Northern Ireland Legal Quarterly 2, 159-182

Walton G, *China’s golden shield: corporations and the development of surveillance technology in the People’s Republic of China*, (International centre for human rights and democratic development, Canada, 2001)

Wang F Y and others, A study of the human flesh search engine: crowd-powered expansion of online knowledge, IEEE Computer Society, August 2010, 45-53

Wang H, *Protecting Privacy in China: A Research on China’s Privacy Standards and the Possibility of Establishing the Right of Privacy and the Information Privacy Protection Legislation in Modern China* (Springer, Berlin, 2011)

Wang S S and Hong J, ‘Discourse behind the Forbidden Realm: Internet surveillance and its implications on China’s blogosphere’, Telematics and Informatics 27 (2010) 67-78

Ward D ‘Sisyphean circles: the Communications Assistance for Law Enforcement Act’ (1996) 22 Rutgers Computer & Technology L.J. 267

Warren S D and Brandies L D, ‘The Right to Privacy’ 4 Harv. L. Rev. 193

Watkins P D, ‘FISA and NSA spying: are there Constitutional implications?’, 3 Homeland Security Rev 125 (2009)

Webster's Third New International Dictionary of the English Language (Bell, 1961)

Weinstein M A, 'The uses of privacy in good life', in Pennock J R and Chapman J W (eds) *Privacy: Nomos XIII* (Atherton, New York, 1971)

Weiss M A and Archick K, U.S.-EU Data Privacy: From Safe Harbor to Privacy Shield, Congressional Research Service, May 19 2016.

Westin A, *Privacy and Freedom* (Athenum, New York, 1970)

Williams E, *China yesterday and to-day* (5th edn. Revised) (Harrap, London, 1932)

Wines M, LaFraniere S and Ansfield J, ‘China’s censors tackle and trip over the Internet’, (*New York Times*, 7 April 2010) <http://www.nytimes.com/2010/04/08/world/asia/08censor.html>

Winfield P H, 'Privacy' (1931) 47 LQR 23

Wing D, ‘Network address translation: extending the Internet address space’, IEEE Internet Computing Vol 14 issue 4, July-August 2010

Wu W, ‘Great leap or long march: some policy issues of the development of the Internet in China’, 20 Telecommunications Policy 9, 699-711, 1996

Xue H, 'Privacy and personal data protection in China: an update for the year end 2009', 26 Computer Law & Security Review 284

Zapotosky M, Lowery W and Berman M, ‘President Trump’s Justice Dept. could see less scrutiny of police, more surveillance of Muslims’, (*Washington Post*, 10 November 2016) <https://www.washingtonpost.com/world/national-security/donald-trump-preached-law-and-order-now-likely-comes-less-police-scrutiny-more-surveillance-of-muslims/2016/11/10/c430a234-a696-11e6-ba59-a7d93165c6d4_story.html?utm_term=.e209a7e9cefb>

Zetter K., ‘World’s Top Surveillance Societies’ <https://www.wired.com/2007/12/worlds-top-surv/>

Zheng Y, *Technological Empowerment: The Internet, State, and Society in China* (Stanford University Press, 2008)

Zhu G, ‘The Right to Privacy: An Emerging Right in Chinese Law’, 18 Statute L. Rev. 3 1997, 208-214

Zimmerman P, Why I wrote PGP <http://www.philzimmermann.com/EN/essays/index.html>

Zittrain J, *The future of the Internet and how to stop it* (Yale University Press, New Haven, 2008)

Zorn W, China’s CSNET Connection 1987 – origin of the China Academic Network CANET <https://www.informatik.kit.edu/downloads/ZornContribution_to_AsiaInternet History-10Jul2012.pdf>